# D-Link ™ DES-3550

## Managed 48-port 10/100Mbps and 2GE ports Layer 2 Ethernet Switch

# *Manual*

**Information in this document is subject to change without notice.**
**© 2005 D-Link Computer Corporation. All rights reserved.**

Reproduction in any manner whatsoever without the written permission of D-Link Computer Corporation is strictly forbidden.

Trademarks used in this text: *D-Link* and the *D-LINK* logo are trademarks of D-Link Computer Corporation; *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

February 2005 P/N 651ES3526015

**FCC Warning**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

**CE Mark Warning**

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

**Warnung!**

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

**Precaución!**

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

**Attention!**

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

**Attenzione!**

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

**VCCI Warning**

この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

**BSMI Warning**

警告使用者
這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,
在這種情況下使用者會被要求採取某些適當的對策

# CONTENTS


**PREFACE** ..... **VIII**

INTENDED READERS ..... VIII

**TYPOGRAPHICAL CONVENTIONS** ..... **VIII**

**NOTES, NOTICES, AND CAUTIONS** ..... **IX**

**SAFETY INSTRUCTIONS** ..... **IX**

*Safety Cautions* ..... *x*

*General Precautions for Rack-Mountable Products* ..... *xi*

*Protecting Against Electrostatic Discharge* ..... *xii*

**INTRODUCTION** ..... **13**

ETHERNET TECHNOLOGY ..... 13

*Fast Ethernet Technology* ..... *13*

*Gigabit Ethernet Technology* ..... *13*

SWITCHING TECHNOLOGY ..... 14

SWITCH DESCRIPTION ..... 14

*Features* ..... *15*

*Ports* ..... *16*

FRONT-PANEL COMPONENTS ..... 17

*LED Indicators* ..... *17*

REAR PANEL DESCRIPTION ..... 18

SIDE PANEL DESCRIPTION ..... 18

GIGABIT COMBO PORTS ..... 18

**INSTALLATION** ..... **20**

*Package Contents* ..... *20*

BEFORE YOU CONNECT TO THE NETWORK ..... 20

INSTALLING THE SWITCH WITHOUT THE RACK ..... 21

INSTALLING THE SWITCH IN A RACK ..... 21

*Mounting the Switch in a standard 19" rack.* ..... *22*

POWER ON ..... 22

*Power Failure* ..... *22*

**CONNECTING THE SWITCH** ..... **23**

SWITCH TO END NODE ..... 23

SWITCH TO HUB OR SWITCH ..... 23

CONNECTING TO NETWORK BACKBONE OR SERVER ..... 24

**INTRODUCTION TO SWITCH MANAGEMENT** ..... **25**

MANAGEMENT OPTIONS ..... 25

*Web-based Management Interface* ..... *25*

*SNMP-Based Management* ..... *25*

*Command Line Console Interface Through The Serial Port* ..... *25*
*Connecting the Console Port (RS-232 DCE)* ..... *25*
*First Time Connecting to The Switch* ..... *27*
PASSWORD PROTECTION ..... 29
*SNMP Settings* ..... *29*
IP ADDRESS ASSIGNMENT ..... 31
CONNECTING DEVICES TO THE SWITCH ..... 32
**INTRODUCTION TO WEB-BASED SWITCH CONFIGURATION ..... 34**
*Web-based User Interface* ..... *35*
**CONFIGURING THE SWITCH ..... 37**
IP ADDRESS ..... 37
SWITCH INFORMATION ..... 40
*Switch Information* ..... *40*
*Advanced Settings* ..... *41*
PORT CONFIGURATIONS ..... 43
PORT MIRRORING ..... 45
PORT DESCRIPTION ..... 46
IGMP ..... 48
*IGMP Snooping* ..... *48*
*Static Router Ports* ..... *49*
SPANNING TREE ..... 51
*802.1w Rapid Spanning Tree* ..... *51*
*STP Switch Settings* ..... *52*
*STP Port Settings* ..... *54*
FORWARDING FILTERING ..... 57
*Unicast Forwarding* ..... *57*
*Static Multicast Forwarding* ..... *57*
*Multicast Port Filtering* ..... *58*
VLANS ..... 60
*Understanding IEEE 802.1p Priority* ..... *60*
*VLANs* ..... *61*
*IEEE 802.1Q VLANs* ..... *61*
*Port-based VLANs* ..... *67*
*Static VLAN Entry* ..... *67*
*Port VLAN ID(PVID)* ..... *70*
PORT BANDWIDTH ..... 71
SNTP SETTINGS ..... 73
*Current Time Settings* ..... *73*
*Time Zone and DST* ..... *74*

PORT SECURITY ..... 76
QOS ..... 78
*Understanding QoS* ..... *78*
*Traffic Control* ..... *79*
*802.1p Default Priority* ..... *79*
*802.1p User Priority* ..... *81*
*Scheduling* ..... *81*
TRAFFIC SEGMENTATION ..... 82
MAC NOTIFICATION ..... 84
*Global Settings* ..... *84*
*Port Settings* ..... *84*
LACP ..... 86
*Understanding Port Trunk Groups* ..... *86*
*LACP Port* ..... *89*
ACCESS PROFILE TABLE ..... 91
CONFIGURING THE ACCESS PROFILE TABLE ..... 91
SYSTEM LOG SERVER ..... 103
PAE ACCESS ENTITY (802.1X) ..... 104
*Understanding 802.1x Port-based Network Access Control* ..... *104*
*Configure Authenticator* ..... *106*
*Port Capability Settings* ..... *109*
*Initializing Ports* ..... *111*
*Reauthenticate Port(s)* ..... *112*
*RADIUS Server* ..... *113*
**MANAGEMENT ..... 115**
SECURITY IP ..... 115
*User Accounts* ..... *115*
ACCESS AUTHENTICATION CONTROL ..... 117
*Policy & Parameters* ..... *118*
*Application's Authentication Settings* ..... *119*
*Authentication Server Group Settings* ..... *119*
*Authentication Server Hosts* ..... *120*
*Login Method Lists* ..... *122*
*Enable Method Lists* ..... *124*
*Local Enable Password* ..... *126*
*Enable Admin* ..... *126*
SNMP ..... 127
SNMP SETTINGS ..... 127
SNMP USER TABLE ..... 129

SNMP VIEW TABLE ..... 131
SNMP GROUP TABLE ..... 132
SNMP COMMUNITY TABLE CONFIGURATION ..... 134
SNMP HOST TABLE ..... 135
SNMP ENGINE ID ..... 136
**MONITORING ..... 137**
PORT UTILIZATION ..... 137
CPU UTILIZATION ..... 138
PACKETS ..... 139
*Received(RX) ..... 139*
*UMB_cast(RX) ..... 141*
*Transmitted (TX) ..... 143*
ERRORS ..... 145
*Received (RX) ..... 145*
*Transmitted (TX) ..... 147*
SIZE ..... 149
MAC ADDRESS ..... 150
IGMP SNOOPING GROUP ..... 152
IGMP SNOOPING FORWARDING ..... 153
VLAN STATUS ..... 153
BROWSE ROUTER PORT ..... 154
PORT ACCESS CONTROL ..... 155
*Authenticator State ..... 155*
**MAINTENANCE ..... 156**
TFTP SERVICES ..... 156
*Download Firmware From TFTP Server ..... 156*
*Download Settings from TFTP Server ..... 157*
*Upload Settings to TFTP Server ..... 157*
*Upload Log to TFTP Server ..... 158*
*Switch History ..... 158*
PING TEST ..... 159
SAVING CHANGES ..... 160
REBOOT SERVICES ..... 161
*Reboot Device ..... 161*
RESET ..... 161
LOGOUT ..... 162
**SINGLE IP MANAGEMENT ..... 163**
SINGLE IP MANAGEMENT (SIM) OVERVIEW ..... 163
SIM USING THE WEB INTERFACE ..... 164

*Topology* ..... *166*
*Tool Tips* ..... *168*
*Right Click* ..... *170*
*Menu Bar* ..... *174*
FIRMWARE UPGRADE ..... 175
CONFIGURATION FILE BACKUP/RESTORE ..... 176
**CABLES AND CONNECTORS ..... 179**
**CABLE LENGTHS ..... 180**
**GLOSSARY ..... 180**

# Preface

The ***DES-3550 Manual*** is divided into sections that describe the system installation and operating instructions with examples.

**Section 1, Introduction** - Describes the Switch and its features.

**Section 2, Installation**– Helps you get started with the basic installation of the Switch and also describes the front panel, rear panel, side panels, and LED indicators of the Switch.
**Section 3, Connecting the Switch** – Tells how you can connect the Switch to your Ethernet/Fast Ethernet network.
**Section 4, Introduction to Switch Management** – Introduces basic Switch management features, including password protection, SNMP settings, IP address assignment, and connecting devices to the Switch.
**Section 5, Introduction to Web-based Switch Management** – Talks about connecting to and using the Web-based switch management feature on the Switch.
**Section 6, Configuring the Switch** – A detailed discussion about configuring some of the basic functions of the Switch, including accessing the Switch information, using the Switch's utilities, and setting up network configurations, such as Quality of Service, The Access Profile Table, port mirroring, and configuring the Spanning Tree.
**Section 7, Management** – A discussion of the security features of the Switch, including Security IP, User Accounts, Access Authentication Control, and SNMP.
**Section 8, Monitoring** – Features graphs and screens used in monitoring features and packets on the Switch.
**Section 9, Maintenance –** Features information on Switch utility functions, including TFTP Services, Switch History, Ping Test Save Changes, and Rebooting Services.
**Section 10, Single IP Management –** Discussion on the Single IP Management function of the Switch, including functions and features of the Java based user interface and the utilities of the SIM function.
**Appendix A, Technical Specifications** – The technical specifications of the DES-3550.
**Appendix B, Cables and Connectors** – Describes the RJ-45 receptacle/connector, straight-through and crossover cables and standard pin assignments.
**Appendix C, Cable Lengths** – Information on cable types and maximum distances.
**Glossary** – Lists definitions for terms and acronyms used in this document.

## Intended Readers

***The DES-3550 Manual*** contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

# Typographical Conventions

| Convention | Description |
|---|---|

| | |
|---|---|
| [ ] | In a command line, square brackets indicate an optional entry. For example: [**copy *filename***] means that optionally you can type copy followed by the name of the file. Do not type the brackets. |
| **Bold font** | Indicates a button, a toolbar icon, menu, or menu item. For example: Open the **File** menu and choose **Cancel**. Used for emphasis. May also indicate system messages or prompts appearing on your screen. For example: You have mail. Bold font is also used to represent filenames, program names and commands. For example: use the **copy** command. |
| **`Boldface Typewriter Font`** | Indicates commands and responses to prompts that must be typed exactly as printed in the manual. |
| Initial capital letter | Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter. |
| *Italics* | Indicates a window name or a field. Also can indicate a variable or parameter that is replaced with an appropriate word or string. For example: type *filename* means that you should type the actual filename instead of the word shown in italic. |
| **Menu Name** > **Menu Option** | Menu Name > Menu Option Indicates the menu structure. **Device > Port > Port Properties** means the Port Properties menu option under the Port menu option that is located under the Device menu. |

# Notes, Notices, and Cautions

**NOTE:** A NOTE indicates important information that helps you make better use of your device.

**NOTICE:** A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

**CAUTION:** A CAUTION indicates a potential for property damage, personal injury, or death.

# Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage. Throughout this safety section, the caution icon ( ) is used to indicate cautions and precautions that you need to review and follow.

## Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions.

Observe and follow service markings. Do not service any product except as explained in your system documentation. Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to an electrical shock. Only a trained service technician should service components inside these compartments.

If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:

  - The power cable, extension cable, or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly, when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause a fire or an electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To help avoid damaging your system, be sure the voltage selection switch (if provided) on the power supply is set to match the power available at your location:
  – 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
  – 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan
  – 230 V/50 Hz in most of Europe, the Middle East, and the Far East
- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent an electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs

to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.

- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
  – Install the power supply before connecting the power cable to the power supply.
  – Unplug the power cable before removing the power supply.
  – If the system has multiple sources of power, disconnect power from the system by unplugging *all* power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

## General Precautions for Rack-Mountable Products

Observe the following precautions for rack stability and safety. Also, refer to the rack installation documentation accompanying the system and the rack for specific caution statements and procedures.

Systems are considered to be components in a rack. Thus, "component" refers to any system as well as to various peripherals or supporting hardware.

**CAUTION:** Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack.
After installing system/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.

- After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any component when servicing other components in a rack.

**NOTE:** A qualified electrician must perform all connections to DC power and to safety grounds. All electrical wiring must comply with applicable local or national codes and practices.

**CAUTION:** Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

**CAUTION:** The system chassis must be positively grounded to the rack cabinet frame. Do not attempt to connect power to the system until grounding cables are connected. Completed power and safety ground wiring must be inspected by a qualified electrical inspector. An energy hazard will exist if the safety ground cable is omitted or disconnected.

## Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads, and an antistatic grounding strap.

# SECTION 1

# Introduction

***Ethernet Technology***
***Switch Description***
***Features***
***Ports***
***Front-Panel Components***
***Side Panel Description***
***Rear Panel Description***
***Gigabit Combo Ports***

## Ethernet Technology

### Fast Ethernet Technology

The growing importance of LANs and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies are proposed to provide greater bandwidth and improve client/server response times. Among them, Fast Ethernet, or 100BASE-T, provides a non-disruptive, smooth evolution from 10BASE-T technology.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet protocol.

### Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full-duplex, flow control, and management objects, but with a tenfold increase in theoretical throughput over 100Mbps Fast Ethernet and a one hundred-fold increase over 10Mbps Ethernet. Since it is compatible with all 10Mbps and 100Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting a company's existing investment in hardware, software, and trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet are essential to coping with the network bottlenecks that frequently develop as computers and their busses get faster and more users use applications that generate more traffic. Upgrading key components, such as your backbone and servers to Gigabit Ethernet can greatly improve network response times as well as significantly speed up the traffic between your subnetworks.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies.

## Switching Technology

Another key development pushing the limits of Ethernet technology is in the field of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by making it possible for a local area network to be divided into different *segments*, which are not competing with each other for network transmission capacity, and therefore decrease the load on each segment.

The Switch acts as a high-speed selective bridge between the individual segments. Traffic that needs to go from one segment to another (from one port to another) is automatically forwarded by the Switch, without interfering with any other segments (ports). This allows the total network capacity to be multiplied, while still maintaining the same network cabling and adapter cards.

For Fast Ethernet or Gigabit Ethernet networks, a switch is an effective way of eliminating problems of chaining hubs beyond the "two-repeater limit." A switch can be used to split parts of the network into different collision domains, for example, making it possible to expand your Fast Ethernet network beyond the 205-meter network diameter limit for 100BASE-TX networks. Switches supporting both traditional 10Mbps Ethernet and 100Mbps Fast Ethernet are also ideal for bridging between existing 10Mbps networks and new 100Mbps networks.

Switching LAN technology is a marked improvement over the previous generation of network bridges, which were characterized by higher latencies. Routers have also been used to segment local area networks, but the cost of a router and the setup and maintenance required make routers relatively impractical. Today's switches are an ideal solution to most kinds of local area network congestion problems.

## Switch Description

The DES-3550 is equipped with unshielded twisted-pair (UTP) cable ports providing dedicated 10 or 100 Mbps bandwidth. The Switch has 24 UTP ports and Auto MDI-X/MDI-II convertible ports that can be used for uplinking to another switch. These ports can be used for connecting PCs, printers, servers, hubs, routers, switches, and other networking devices. The dual speed ports use standard twisted-pair cabling and are ideal for segmenting networks into small, connected subnetworks for superior performance. Each 10/100 port can support up to 200 Mbps of throughput in full-duplex mode.

In addition, the Switch has two Mini-GBIC combo ports. These two, gigabit combo ports are ideal for connecting to a server or network backbone.

This stand-alone Switch enables the network to use some of the most demanding multimedia and imaging applications concurrently with other user applications without creating bottlenecks. The built-in console interface can be used to configure the Switch's settings for priority queuing, VLANs, and port trunk groups, port monitoring, and port speed.

## Features

- IEEE 802.3 10BASE-T compliant
- IEEE 802.3u 100BASE-TX compliant
- IEEE 802.1p Priority Queues
- IEEE 802.3x flow control in full-duplex mode
- IEEE 802.3ad Link Aggregation Control Protocol support.
- IEEE 802.1x Port-based and MAC-based Access Control
- IEEE 802.1Q VLAN
- IEEE 802.1D Spanning Tree and IEEE 802.1W Rapid Spanning Tree support
- Access Control List (ACL) support
- Single IP Management support
- Access Authentication Control utilizing TACACS, XTACACS, and TACACS+
- Dual Image Firmware
- Simple Network Time Protocol support
- MAC Notification support
- Asymmetric VLAN support
- System and Port Utilization support
- System Log Support
- High performance switching engine performs forwarding and filtering at full wire speed, maximum 14, 881 packets/sec on each 10Mbps Ethernet port, and maximum 148,810 packet/sec on 100Mbps Fast Ethernet port.
- Full- and half-duplex for both 10Mbps and 100Mbps connections. Full-duplex allows the switch port to simultaneously transmit and receive data. It only works with connections to full-duplex-capable end stations and switches. Connections to a hub must take place at half-duplex.
- Supports broadcast storm filtering
- Non-blocking store and forward switching scheme capability to support rate adaptation and protocol conversion
- Supports by-port Egress/Ingress rate control.
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed
- Supports port-based enable and disable

- Address table: Supports up to 8K MAC addresses per device
- Supports a packet buffer of up to 64 Megabytes
- Supports Port-based VLAN Groups
- Port Trunking with flexible load distribution and fail-over function
- Supports IGMP Snooping
- Supports SNMP
- Supports Port Mirroring
- MIB support for:
    - RFC1213 MIB II
    - RFC1493 Bridge
    - RFC1757 RMON
    - RFC1643 Ether-like MIB
    - RFC2233 Interface MIB
    - Private MIB
    - RFC2674 for 802.1p
    - IEEE 802.1x MIB
- RS-232 DCE console port for Switch management
- Provides parallel LED display for port status such as link/act, speed, etc.

## Ports

- Forty-eight (48) high-performance (MDI-X/MDI-II) ports for connecting to end stations, servers, hubs, and other networking devices.
- All UTP ports can auto-negotiate between 10Mbps and 100Mbps, half-duplex and full-duplex, and feature flow control.
- Two 1000BASE-T Mini-GBIC combo ports for connecting to another switch, server, or network backbone.
- RS-232 DCE Diagnostic port (console port) for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.

### Important Note:

For customers interested in D-View, D-Link Corporation's proprietary SNMP management software, go to the D-Link Website (www.dlink.com.cn) and download the software and manual.

# Front-Panel Components

The front panel of the Switch consists of LED indicators for power and for each 10/100 Mbps twisted-pair ports, and two 1000BASE-T Mini-GBIC ports.

### DES-3550

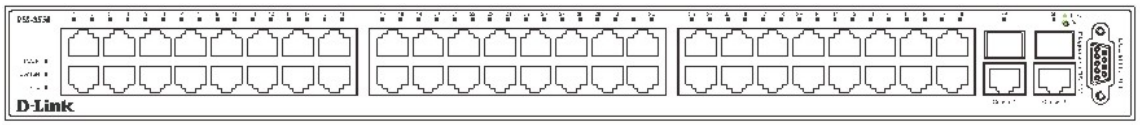


**Figure 1- 1. Front Panel View of the DES-3550 as shipped**

Comprehensive LED indicators display the status of the Swtch and the network.

## LED Indicators

The LED indicators of the Switch include **Power**, **Console**, **Link/Act**, **Speed**, and **FDX.** This Switch also includes a **LED Mode** button, which has the default setting set to **Link/Act**. The user may scroll through to show the LED status for **Link/Act**, **Speed**, and **FDX** of each port. The following shows the LED indicators for the Switch along with an explanation of each indicator.

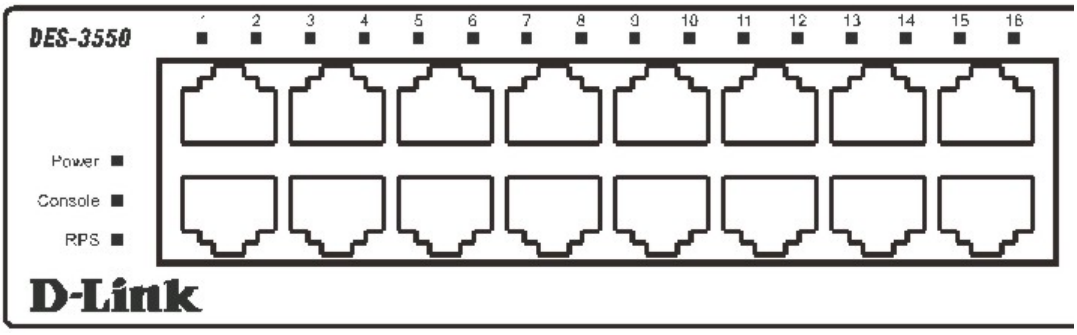



**Figure 1- 2. LED Indicators**

| | |
|---|---|
| **Power** | This LED will light green after the Switch is powered on to indicate the ready state of the device. The indicator is dark when the Switch is powered off. |
| **Console** | This LED should blink during the Power-On Self Test (POST). When the POST is finished, the LED goes dark. This indicator is lit solid green when the Switch is being logged into via out-of-band/local console management through the RS-232 console port in the back of the Switch using a straight-through serial cable. |
| **RPS** | This LED will be lit when the redundant power supply is present and in use. Otherwise, it will remain dark. |
| **Port LEDs** | One row of LEDs for each port is located above the ports on the front panel. The first LED is for the top port and the second one is for the bottom ports. The LED will light green when there is a secure connection to a device from the corresponding port. This LED will blink when there is activity on the port. |
| **Gigabit Ports** | The Switch's two Mini GBIC ports have their own corresponding LEDs. The LED will light green when there is a secure connection to a device from the corresponding port. This LED will blink when there is activity on the port. |

## Rear Panel Description

The rear panel of the Switch contains an AC power connector.

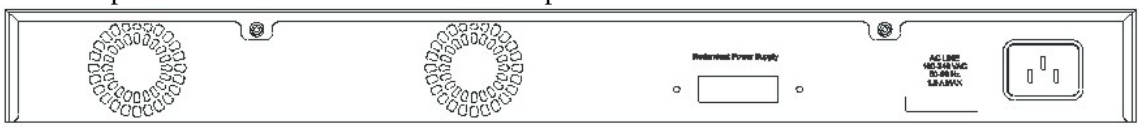


**Figure 1- 3. Rear panel view of the Switch**

The AC power connector is a standard three-pronged connector that supports the power cord. Plug in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. The Switch automatically adjusts its power setting to any supply voltage in the range from 100 ~ 240 VAC at 50 ~ 60 Hz.

The rear panel also includes an outlet for an optional external power supply. When power fails, the optional external RPS will take over all the power immediately and automatically.

The rear panel contains two system fans. The system fans are used to dissipate heat. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the Switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

## Side Panel Description

The right-hand side panel of the Switch contains heat vents to dissipate heat. Keep these openings clear of obstructions of up to six inches of space. Failure to comply with this may result in the system overheating and eventually to a system failure.

**Figure 1-4. Side Panels**

## Gigabit Combo Ports

In addition to the 48 10/100 Mbps ports, the Switch features two **Gigabit Ethernet Combo** ports. These two ports are 1000BASE-T copper ports (provided) and Mini-GBIC ports (optional). See the diagram below to view the two Mini-GBIC port modules being plugged into the Switch. Please note that although these two front panel modules can be used simultaneously, the ports must be different. The GBIC port will always have the highest priority.

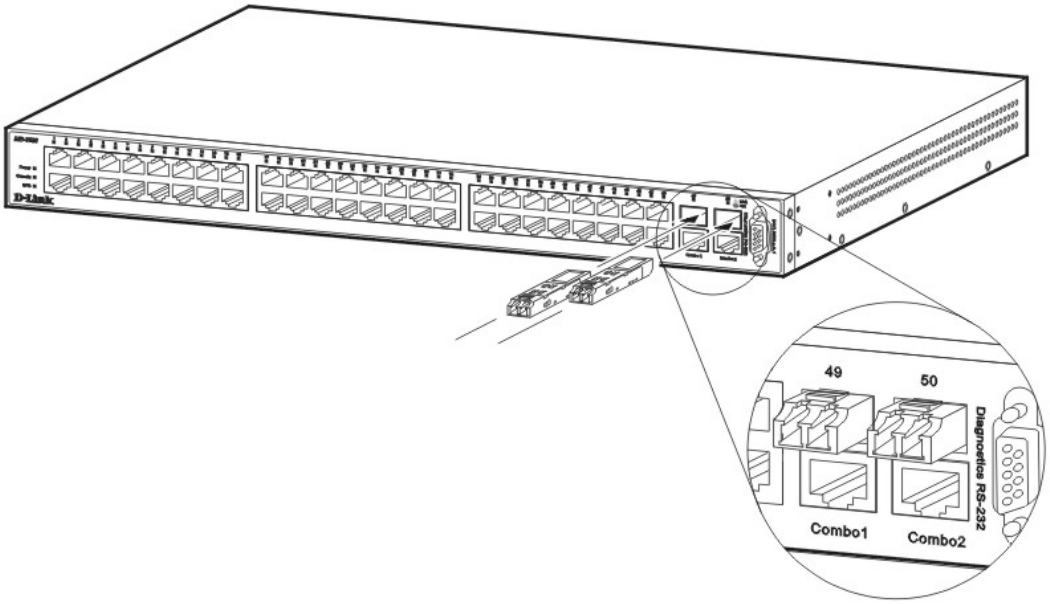



**Figure 1- 5. Mini-GBIC modules plug-in to the Switch**

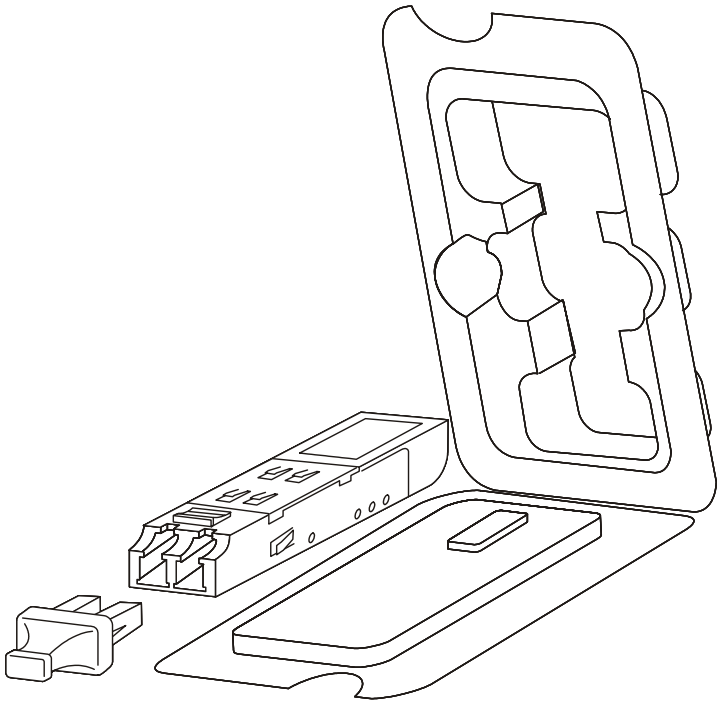


**Figure 1- 6. Installing the Mini-GBIC Module**

SECTION 2

# Installation

***Package Contents***
***Before You Connect to the Network***
***Installing the Switch Without the Rack***
***Rack Installation***
***Power On***

## Package Contents

Open the shipping carton of the Switch and carefully unpack its contents. The carton should contain the following items:

- One DES-3550 Stand-alone Switch
- One AC power cord
- This Manual
- Registration card
- Mounting kit (two brackets and screws)
- Four rubber feet with adhesive backing
- RS-232 console cable

If any item is found missing or damaged, please contact your local D-Link Reseller for replacement.

## Before You Connect to the Network

The site where you install the Switch may greatly affect its performance. Please follow these guidelines for setting up the Switch.

- Install the Switch on a sturdy, level surface that can support at least 3 kg (6.6 lb) of weight. Do not place heavy objects on the Switch.
- The power outlet should be within 1.82 meters (6 feet) of the Switch.
- Visually inspect the power cord and see that it is fully secured to the AC power port.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch. Leave at least 15 cm (6 inches) of space at the front and rear of the Switch for ventilation.
- Install the Switch in a fairly cool and dry place for the acceptable temperature and humidity operating ranges.
- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.

- When installing the Switch on a level surface, attach the rubber feet to the bottom of the device. The rubber feet cushion the Switch, protect the casing from scratches, and prevent it from scratching other surfaces.

## Installing the Switch Without the Rack

When installing the Switch on a desktop or shelf, the rubber feet included with the Switch should first be attached. Attach these cushioning feet on the bottom at each corner of the device. Allow enough ventilation space between the Switch and any other objects in the vicinity.

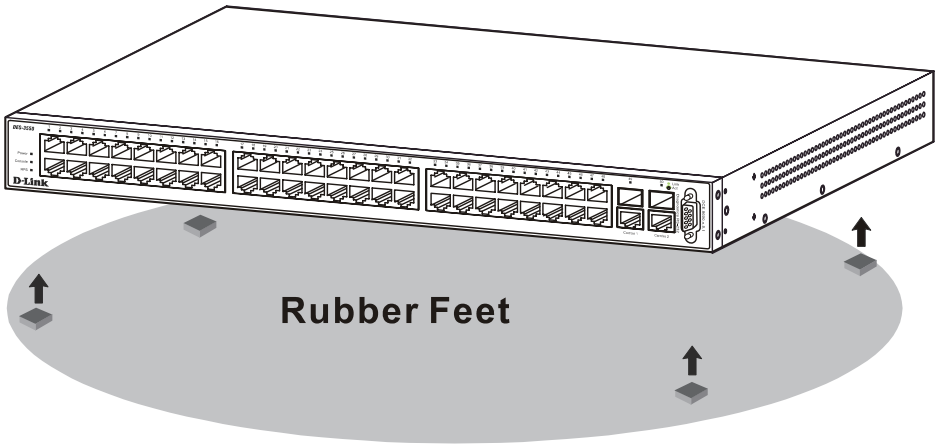



**Figure 2- 1. Prepare Switch for installation on a desktop or shelf**

## Installing the Switch in a Rack

The Switch can be mounted in a standard 19" rack. Use the following diagrams to guide you.

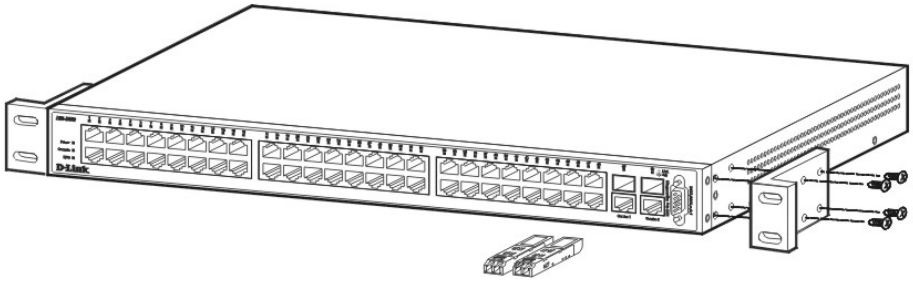


**Figure 2- 2. Fasten mounting brackets to Switch**

Fasten the mounting brackets to the Switch using the screws provided. With the brackets attached securely, you can mount the Switch in a standard rack as shown in Figure 2-3, below.

### Mounting the Switch in a standard 19" rack.

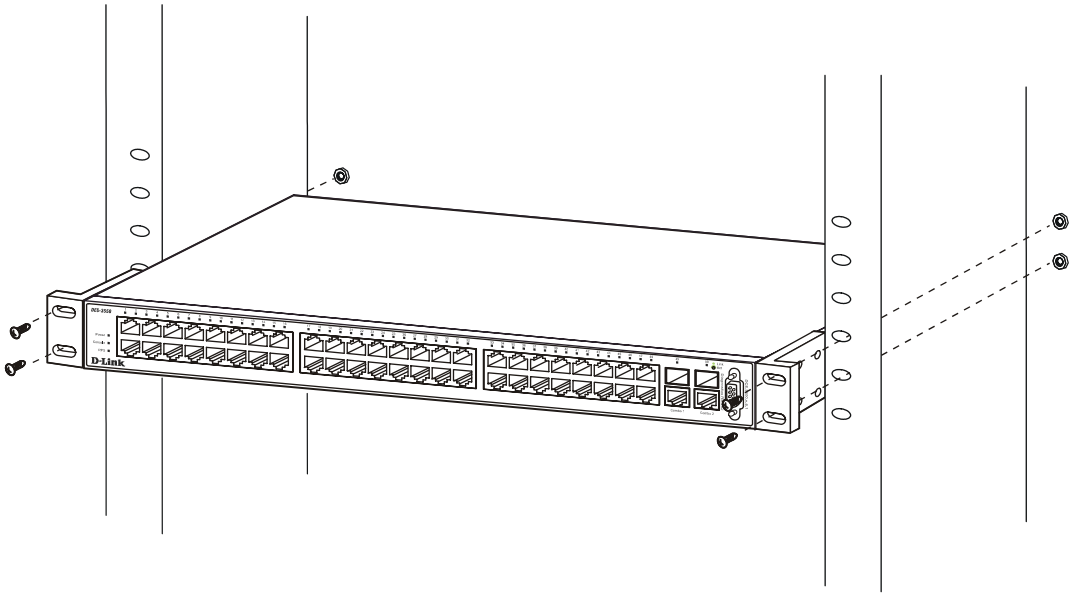


**Figure 2- 3. Installing Switch in a rack**

## Power On

Plug one end of the AC power cord into the power connector of the Switch and the other end into the local power source outlet.

After the Switch is powered on, the LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.

### Power Failure

As a precaution, in the event of a power failure, unplug the Switch. When power is resumed, plug the Switch back in.

**Section 3**

# Connecting The Switch

***Switch To End Node***
***Switch To Hub or Switch***
***Connecting To Network Backbone or Server***

**NOTE:** All 48 high-performance NWay Ethernet ports can support both MDI-II and MDI-X connections.

## Switch To End Node

End nodes include PCs outfitted with a 10, 100, or 1000 Mbps RJ-45 Ethernet/Fast Ethernet Network Interface Card (NIC) and most routers.

An end node can be connected to the Switch via a twisted-pair Category 3, 4, or 5 UTP/STP cable. The end node should be connected to any of the ports of the Switch.

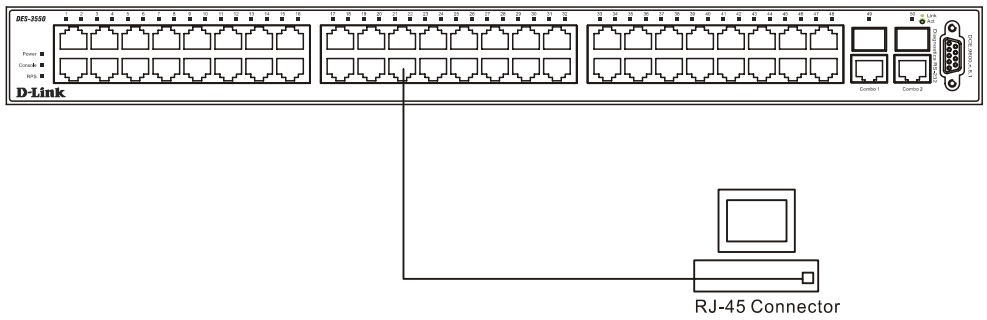



**Figure 3- 1. Switch connected to an end node**

The **Link/Act** LEDs for each UTP port will light green or amber when the link is valid. A blinking LED indicates packet activity on that port.

## Switch to Hub or Switch

These connections can be accomplished in a number of ways using a normal cable.

- A 10BASE-T hub or switch can be connected to the Switch via a twisted-pair Category 3, 4, or 5 UTP/STP cable.
- A 100BASE-TX hub or switch can be connected to the Switch via a twisted -pair Category 5 UTP/STP cable.

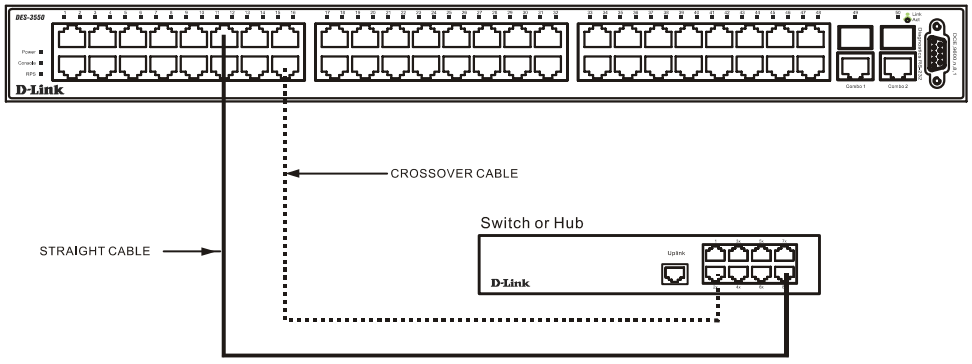



**Figure 3- 2. Switch connected to a port on a hub or switch using either a straight or crossover cable– any normal cable is fine**

## Connecting To Network Backbone or Server

The two Mini-GBIC combo ports are ideal for uplinking to a network backbone or server. The copper ports operate at a speed of *1000, 100, or 10Mbps* in *ful-l or half-duplex mode*. The fiber optic ports can operate at 1000Mbps in full-duplex mode.
Connections to the Gigabit Ethernet ports are made using fiber optic cable or Category 5 copper cable, depending on the type of port. A valid connection is indicated when the Link LED is lit.

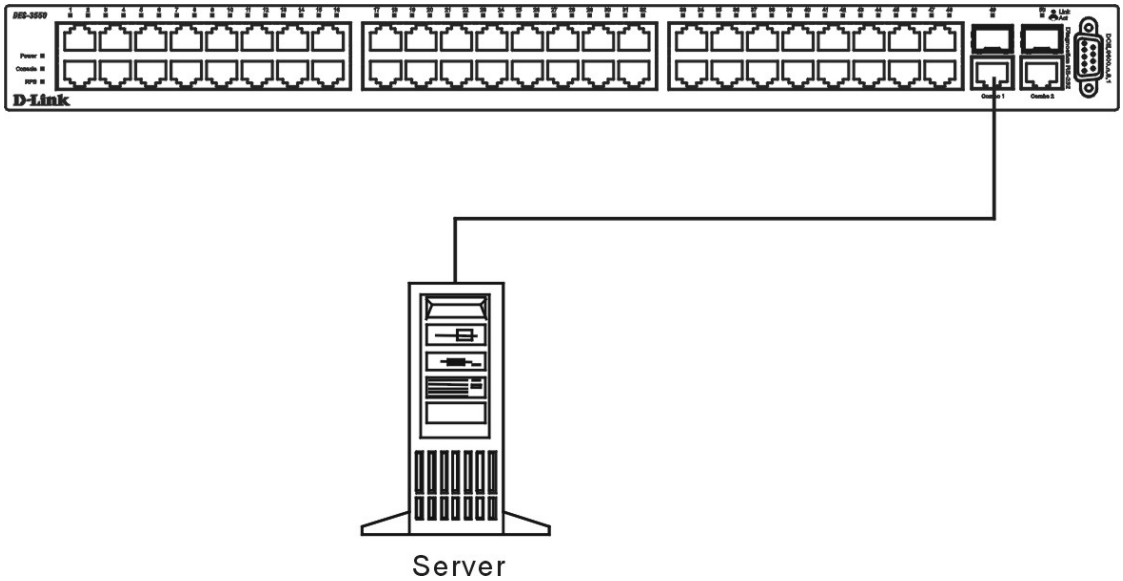



**Figure 3- 3. Uplink Connection to a server.**

# Section 4

# Introduction To Switch Management

***Management Options***
***Web-based Management Interface***
***SNMP-Based Management***
***Managing User Accounts***
***Command Line Console Interface Through The Serial Port***
***Connecting the Console Port (RS-232 DCE)***
***First Time Connecting to The Switch***
***Password Protection***
***SNMP Settings***
***IP Address Assignment***
***Connecting Devices to the Switch***

## Management Options

This system may be managed out-of-band through the console port on the front panel or in-band using Telnet. The user may also choose the Web-based management, accessible through a Web browser.

### Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a Web browser, such as Netscape Navigator (version 6.2 and higher) or Microsoft® Internet Explorer (version 5.0).

### SNMP-Based Management

You can manage the Switch with an SNMP-compatible console program. The Switch supports SNMP version 1.0, version 2.0, and version 3.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

### Command Line Console Interface Through the Serial Port

You can also connect a computer or terminal to the serial console port to access the Switch. The command-line-driven interface provides complete access to all Switch management features.

### Connecting the Console Port (RS-232 DCE)

The Switch provides an RS-232 serial port that enables a connection to a computer or terminal for monitoring and configuring the Switch. This port is a female DB-9 connector, implemented as a data terminal equipment (DTE) connection.

**To use the console port, you need the following equipment:**

- A terminal or a computer with both a serial port and the ability to emulate a terminal.
- A null modem or crossover RS-232 cable with a female DB-9 connector for the console port on the Switch.

**To connect a terminal to the console port:**

1. Connect the female connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.
2. Connect the other end of the cable to a terminal or to the serial connector of a computer running terminal emulation software. Set the terminal emulation software as follows:
    1. Select the appropriate serial port (COM port 1 or COM port 2).
    3. Set the data rate to 9600 baud.
    4. Set the data format to 8 data bits, 1 stop bit, and no parity.
    5. Set flow control to `none`.
    6. Under **Properties**, select **VT100 for Emulation** mode.
    7. Select **Terminal keys** for **Function, Arrow, and Ctrl keys**. Ensure that you select **Terminal keys** (*not* **Windows keys**).

**NOTICE:** When you use HyperTerminal with the Microsoft® Windows® 2000 operating system, ensure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 allows you to use arrow keys in HyperTerminal's VT100 emulation. See **www.microsoft.com** for information on Windows 2000 service packs.

    8. After you have correctly set up the terminal, plug the power cable into the power receptacle on the back of the Switch. The boot sequence appears in the terminal.
    9. After the boot sequence completes, the console login screen displays.
    10. If you have not logged into the command line interface (CLI) program, press the Enter key at the User name and password prompts. There is no default user name and password for the Switch. User names and passwords must first be created by the administrator. If you have previously set up user accounts, log in and continue to configure the Switch.
    11. Enter the commands to complete your desired tasks. Many commands require administrator-level access privileges. Read the next section for more information on setting up user accounts. See the *DES-3550 Command Line Interface Reference Manual* on the documentation CD for a list of all commands and additional information on using the CLI.

When you have completed your tasks, exit the session with the **`logout`** command or close the emulator program.

Make sure the terminal or PC you are using to make this connection is configured to match these settings.

If you are having problems making this connection on a PC, make sure the emulation is set to VT-100. You will be able to set the emulation by clicking on the **File** menu in your HyperTerminal window, clicking on **Properties** in the drop-down menu, and then clicking the

**Settings** tab. This is where you will find the **Emulation** options. If you still do not see anything, try rebooting the Switch by disconnecting its power supply.

Once connected to the console, the screen below will appear on your console screen. This is where the user will enter commands to perform all the available management functions. The Switch will prompt the user to enter a user name and a password. Upon the initial connection, there is no user name or password and therefore just press enter twice to access the command line interface.

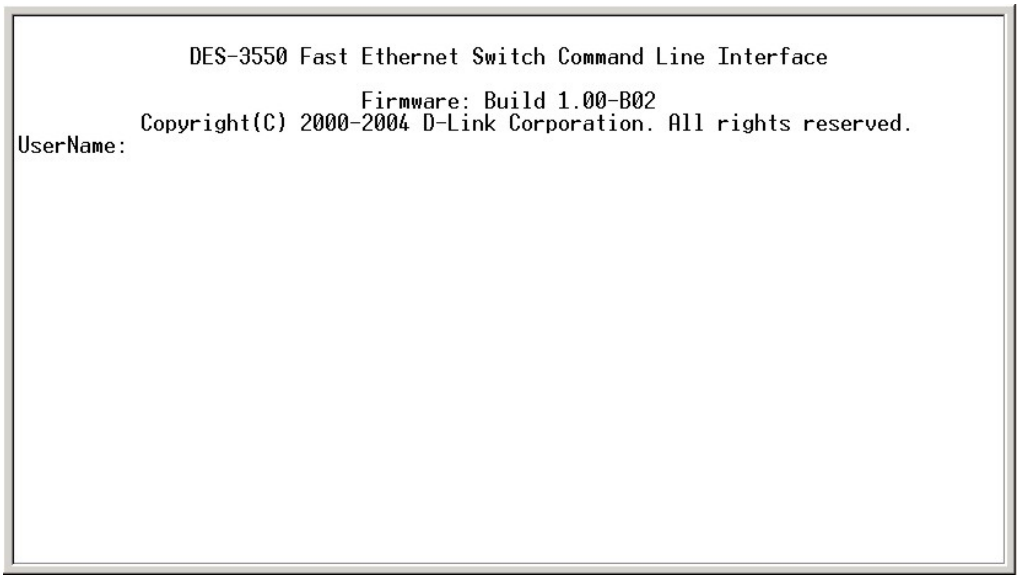

DES-3550 Fast Ethernet Switch Command Line Interface
Firmware: Build 1.00-B02
Copyright(C) 2000-2004 D-Link Corporation. All rights reserved.
UserName:

**Figure 4- 1. Initial screen after first connection.**

## First Time Connecting to the Switch

The Switch supports user-based security that can allow you to prevent unauthorized users from accessing the Switch or changing its settings. This section tells how to log onto the Switch.

**NOTE:** The passwords used to access the Switch are case-sensitive; therefore, "S" is not the same as "s."

When you first connect to the Switch, you will be presented with the first login screen (shown below).

**NOTE:** Press Ctrl+R to refresh the screen. This command can be used at any time to force the console program in the Switch to refresh the console screen.

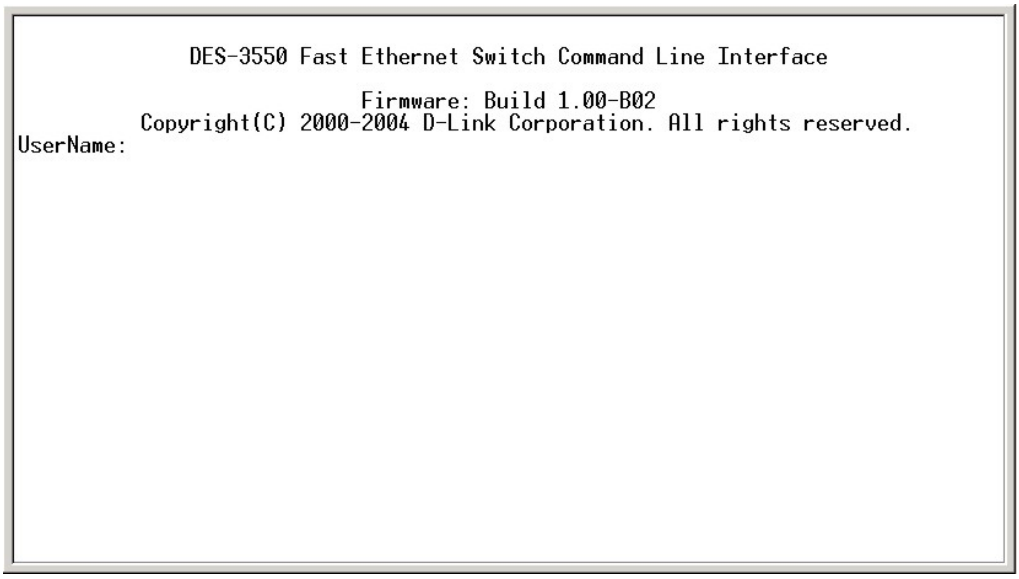

DES-3550 Fast Ethernet Switch Command Line Interface
Firmware: Build 1.00-B02
Copyright(C) 2000-2004 D-Link Corporation. All rights reserved.
UserName:

**Figure 4- 2. Initial screen, first time connecting to the Switch**

Press **Enter** in both the Username and Password fields. You will be given access to the command prompt **DES-3550:4#** shown below:

There is no initial username or password. Leave the **Username** and **Password** fields blank.

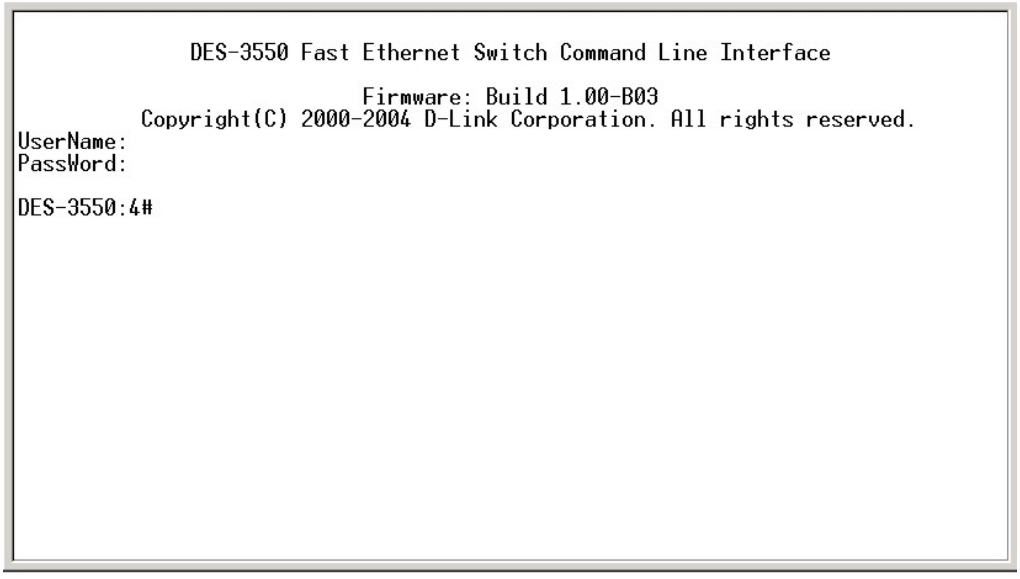



**Figure 4- 3. Command Prompt**

**Note**: The first user automatically gets Administrator level privileges. It is recommended to create at least one Admin-level user account for the Switch.

# Password Protection

The DES-3550 does not have a default user name and password. One of the first tasks when settings up the Switch is to create user accounts. If you log in using a predefined administrator-level user name, you have privileged access to the Switch's management software.

After your initial login, define new passwords for both default user names to prevent unauthorized access to the Switch, and record the passwords for future reference.

To create an administrator-level account for the Switch, do the following:

1. At the CLI login prompt, enter **create account admin** followed by the <user name> and press the Enter key.
2. You will be asked to provide a password. Type the <password> used for the administrator account being created and press the Enter key.
3. You will be prompted to enter the same password again to verify it. Type the same password and press the Enter key.
4. Successful creation of the new administrator account will be verified by a **Success** message.

User names and passwords can be up to 15 characters in length.

**NOTE:** Passwords are case sensitive.

The sample below illustrates a successful creation of a new administrator-level account with the user name "newmanager."

```
DES-3550:4#create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password:********
Enter the new password again for confirmation:********

Success.

DES-3550:4#
```

**NOTICE:** CLI configuration commands only modify the running configuration file and are not saved when the Switch is rebooted. To save all your configuration changes in nonvolatile storage, you must use the **save** command to copy the running configuration file to the startup configuration.

## SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other

network devices. Use SNMP to configure system features for proper operation, monitor performance, and detect potential problems in the Switch, switch group, or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The DES-3550 supports SNMP versions 1, 2c, and 3. You can specify which version of SNMP you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

**public** - Allows authorized management stations to retrieve MIB objects.
**private** - Allows authorized management stations to retrieve and modify MIB objects.

SNMP V3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMP v.1 while assigning a higher level of security to another group, granting read/write privileges using SNMP v.3.

Using SNMP v.3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMP v.3 in that SNMP messages may be encrypted. To read more about how to configure SNMP v.3 settings for the Switch read the section entitled **Management**.

### Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change, and Broadcast\Multicast Storm.

### MIBs

Management and counter information are stored by the Switch in the Management Information Base (MIB). The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. The proprietary MIB may also be retrieved by specifying the MIB Object Identifier. MIB values can be either read-only or read-write.

## IP Address Assignment

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found by entering the command "*show switch*" into the command line interface, as shown below.

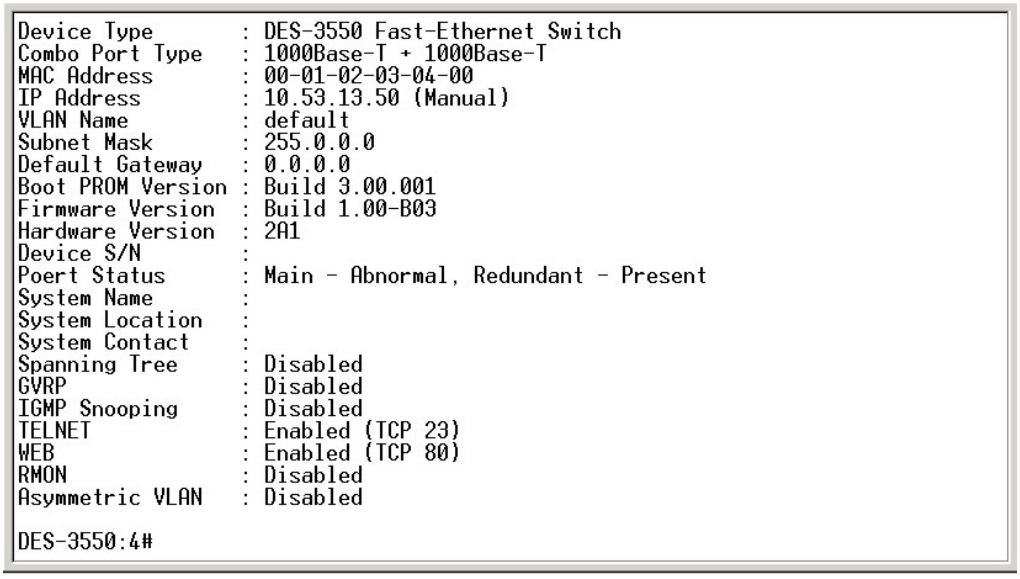

Device Type : DES-3550 Fast-Ethernet Switch
Combo Port Type : 1000Base-T + 1000Base-T
MAC Address : 00-01-02-03-04-00
IP Address : 10.53.13.50 (Manual)
VLAN Name : default
Subnet Mask : 255.0.0.0
Default Gateway : 0.0.0.0
Boot PROM Version : Build 3.00.001
Firmware Version : Build 1.00-B03
Hardware Version : 2A1
Device S/N :
Poert Status : Main - Abnormal, Redundant - Present
System Name :
System Location :
System Contact :
Spanning Tree : Disabled
GVRP : Disabled
IGMP Snooping : Disabled
TELNET : Enabled (TCP 23)
WEB : Enabled (TCP 80)
RMON : Disabled
Asymmetric VLAN : Disabled
DES-3550:4#

**Figure 4- 4. Show switch command**

The Switch's MAC address can also be found from the Web management program on the Switch Information (Basic Settings) window on the Configuration menu.
The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.
The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

1. Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address

to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.

2. Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

The IP interface named **System** on the Switch can be assigned an IP address and subnet mask, which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

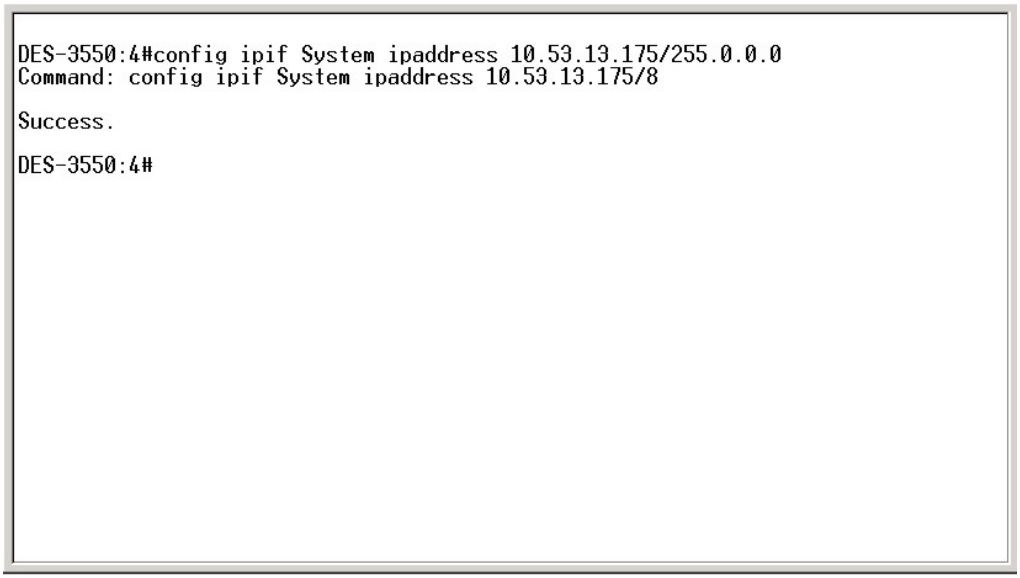



**Figure 4- 5. Assigning the Switch an IP Address**

In the above example, the Switch was assigned an IP address of 10.53.13.175 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management.

## Connecting Devices to the Switch

After you assign IP addresses to the Switch, you can connect devices to the Switch.

To connect a device to an SFP transceiver port:

1. Use your cabling requirements to select an appropriate SFP transceiver type.
2. Insert the SFP transceiver (sold separately) into the SFP transceiver slot.
3. Use the appropriate network cabling to connect a device to the connectors on the SFP transceiver.

**NOTICE:** When the SFP transceiver acquires a link, the associated integrated 10/100/1000BASE-T port is disabled.

# Section 5

# Introduction to Web-based Switch Configuration

***Introduction***
***Login To Web manager***
***Web-Based User Interface***
***Basic Setup***
***Reboot***
***Basic Switch Setup***
***Network Management***
***Switch Utilities***
***Network Monitoring***
***IGMP Snooping Status***

## Introduction

All software functions of the DES-3550 can be managed, configured, and monitored via the embedded web-based (HTML) interface. The Switch can be managed from remote stations anywhere on the network through a standard browser such as Netscape Navigator/Communicator or Microsoft Internet Explorer. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

## Login to Web Manager

To begin managing your Switch, simply run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the Switch.

**NOTE:** The Factory default IP address for the Switch is 10.90.90.90.

In the page that opens, click on the **Login to make a setup** button:

**Figure 5- 1. Login Button**

This opens the management module's user authentication window, as seen below.

Leave both the **User Name** field and the **Password** field blank and click OK. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

## Web-based User Interface

The user interface provides access to various Switch configuration and management screens, allows you to view performance statistics, and permits you to graphically monitor the system status.

### Areas of the User Interface

The figure below shows the user interface. The user interface is divided into 3 distinct areas as described in the table.

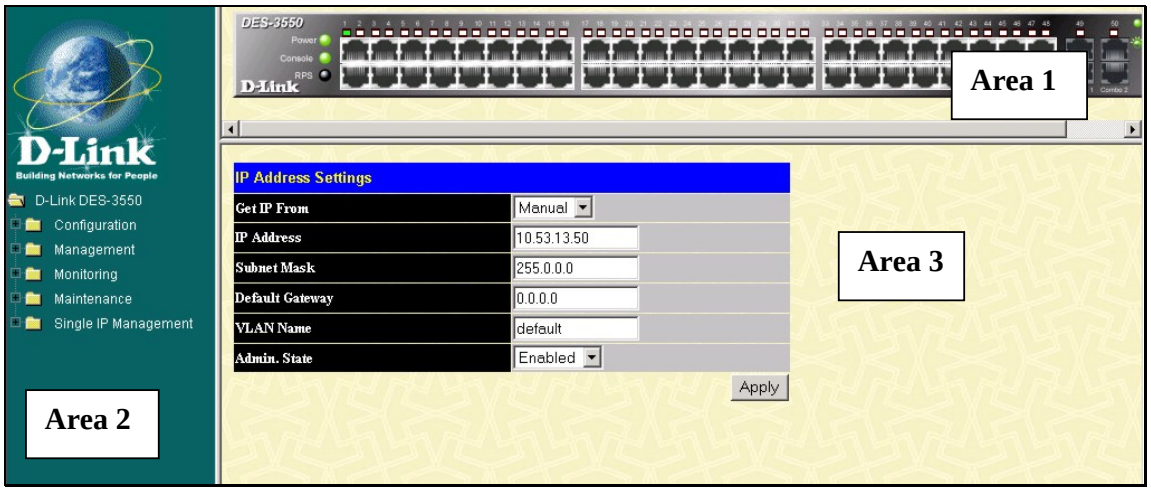



**Figure 5- 2. Main Web-Manager Screen**

| Area | Function |
|---|---|
| 1 | Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode.<br>Various areas of the graphic can be selected for performing management functions, including port configuration. |
| 2 | Select the menu or window to be displayed. The folder icons can be opened to display the hyperlinked menu buttons and subfolders contained within them. Click the D-Link logo to go to the D-Link website. |
| 3 | Presents switch information based on your selection and the entry of configuration data. |

**NOTICE:** Any changes made to the Switch configuration during the current session must be saved in the **Save Changes** web menu (explained below) or use the command line interface (CLI) command **save**.

## Web Pages

When you connect to the management mode of the Switch with a Web browser, a login screen is displayed. Enter a user name and password to access the Switch's management mode. Below is a list and description of the main folders available in the web interface:

**Configurations –** Contains screens concerning configurations for *IP Address, Switch Information, Advanced Settings, Port Configuration, IGMP, Spanning Tree, Forwarding Filtering, VLANs, Port Bandwidth, SNTP Settings, Port Security, QoS, MAC Notification, LACP, Access Profile Table, System Log Servers,* and *PAE Access Entity*

**Management –** Contains screens concerning configurations for *Security IP, User Accounts, Access Authentication Control (TACACS),* and *SNMP V3.*

**Monitoring -** Contains screens concerning monitoring the Switch, pertaining to *Port Utilization, CPU Utilization, Packets, Errors Size, MAC Address, IGMP Snooping Group, IGMP Snooping Forwarding, VLAN Status, Router Port,* and *Port Access Control.*

**Maintenance -** Contains screens concerning configurations and information about Switch maintenance, including *TFTP Services, Switch History, Ping Test, Save Changes, Reboot Services,* and *Logout.*

**Single IP Management –** Contains screens concerning information on Single IP Management, including SIM Settings, Topology, and Firmware/Configuration downloads.

**NOTE:** Be sure to configure the user name and password in the User Accounts menu before connecting the Switch to the greater network.

Section 6

# Configuring The Switch

***IP Address***
***Switch Information***
***Advanced Settings***
***Port Configuration***
***Port Mirroring***
***Port Description***
***IGMP***
***Spanning Tree***
***Forward Filtering***
***VLANs***
***Port Bandwidth***
***SNTP Settings***
***Port Security***
***QoS***
***MAC Notification***
***LACP***
***Access Profile Table***
***System Log Servers***
***PAE Access Entity***

## IP Address

The **IP Address** may initially be set using the console interface prior to connecting to it through the Ethernet. If the Switch IP address has not yet been changed, read the Introduction of the CLI Manual or return to Section 4 of this manual for more information.

To change IP settings using the Web manager you must access the **IP Address** menu located in the **Configuration** folder.

***To configure the Switch's IP address:***
Open the **Configuration** folder and click the **IP Address** menu link. The Web manager will display the Switch's current IP settings in the IP configuration menu, as seen below.

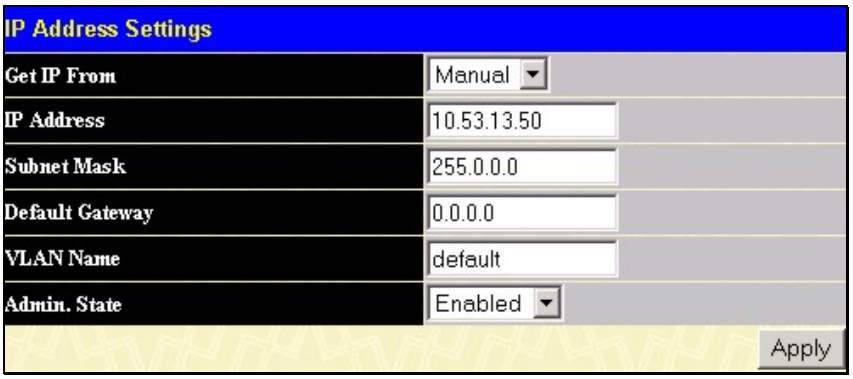



**Figure 6- 1. IP Address Settings window.**

To manually assign the Switch's IP address, subnet mask, and default gateway address:

- Select **Manual** from the **Get IP From** drop-down menu.
- Enter the appropriate IP address and subnet mask.
- If you want to access the Switch from a different subnet from the one it is installed on, enter the IP address of the gateway. If you will manage the Switch from the subnet on which it is installed, you can leave the default address (0.0.0.0) in this field.
- If no VLANs have been previously configured on the Switch, you can use the default VLAN Name (default). The default VLAN contains all of the switch ports as members. If VLANs have been previously configured on the Switch, you will need to enter the VLAN ID of the VLAN that contains the port connected to the management station that will access the Switch. The Switch will allow management access from stations with the same VID listed here.

**NOTE:** The Switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

***To use the***

***BOOTP or DHCP protocols to assign the Switch an IP address, subnet mask, and default gateway address:***

Use the **Get IP From: <Manual>** pull-down menu to choose from **BOOTP** or **DHCP**. This selects how the Switch will be assigned an IP address on the next reboot.

The IP Address Settings options are:

| Parameter | Description |
|---|---|
| **BOOTP** | The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings. |
| **DHCP** | The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings. |
| **Manual** | Allows the entry of an IP address, Subnet Mask, and a Default Gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator. The fields that require entries under this option are as follows: |
| **Subnet Mask** | A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed. |
| **Default Gateway** | IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged. |
| **VLAN Name** | This allows the entry of a VLAN Name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the Security IP Management menu. If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Security IP Management table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP Addresses are assigned. |
| **Admin State** | This field will allow the user the enable or disable the Admin state for the IP interface, by the using the pull-down menu. Disabling this feature will render all remote management inoperable, and thus the only way to configure the Switch will be to use the Console port for the Command Line Interface. |

Click *Apply* to make your changes take effect.

**Setting the Switch's IP Address using the Console Interface**

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.
The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.
The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:
Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.
Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.
The IP interface named **System** on the Switch can be assigned an IP address and subnet mask, which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.
The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

# Switch Information

Click the **Switch Information** link in the **Configuration** menu.
The subsections below describe how to change some of the basic settings for the Switch such as changing IP settings and assigning user names and passwords for management access privileges, as well as how to save the changes and restart the Switch.

## Switch Information

Click the **Switch Information** link in the **Configuration** menu.

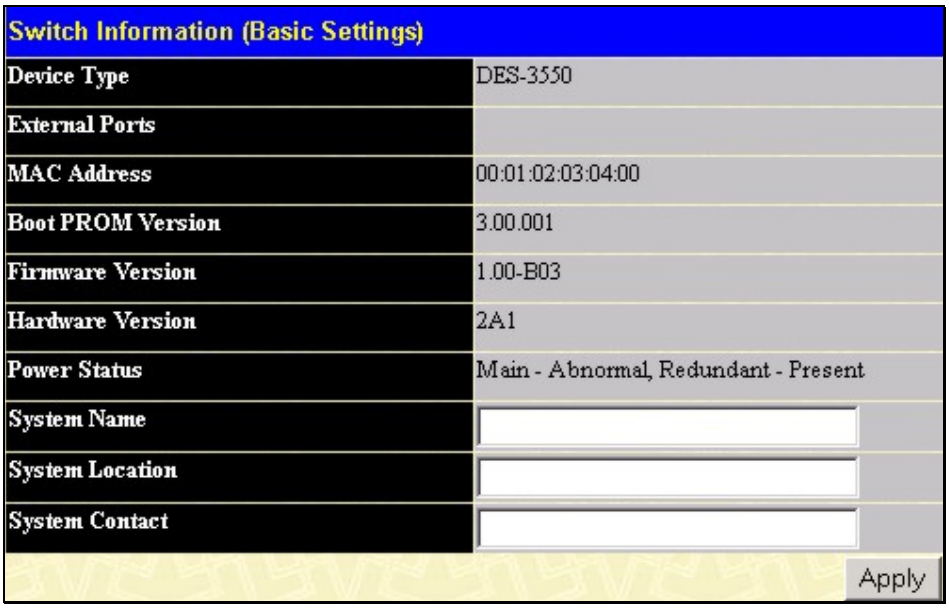



**Figure 6- 2. Switch Information – Basic Settings**

The **Switch Information** window shows the Switch's **MAC Address** (assigned by the factory and is unchangeable), IP configuration, some important functions implemented, and their status. In addition, the **Boot PROM**, **Firmware Version**, and **Hardware Version** are present. This information is helpful to keep track of PROM and Firmware updates and to obtain the Switch's MAC address for entry into another network device's address table, if necessary. The user may also enter a **System Name**, **System Location**, and **System Contact** to aid in defining the Switch, to the user's preference.

## Advanced Settings

The **Advanced Settings** window contains the main settings for all major functions for the Switch. To view the **Advanced Settings** window, click its link in the **Configuration** folder. This will enable the following window to be viewed and configured.

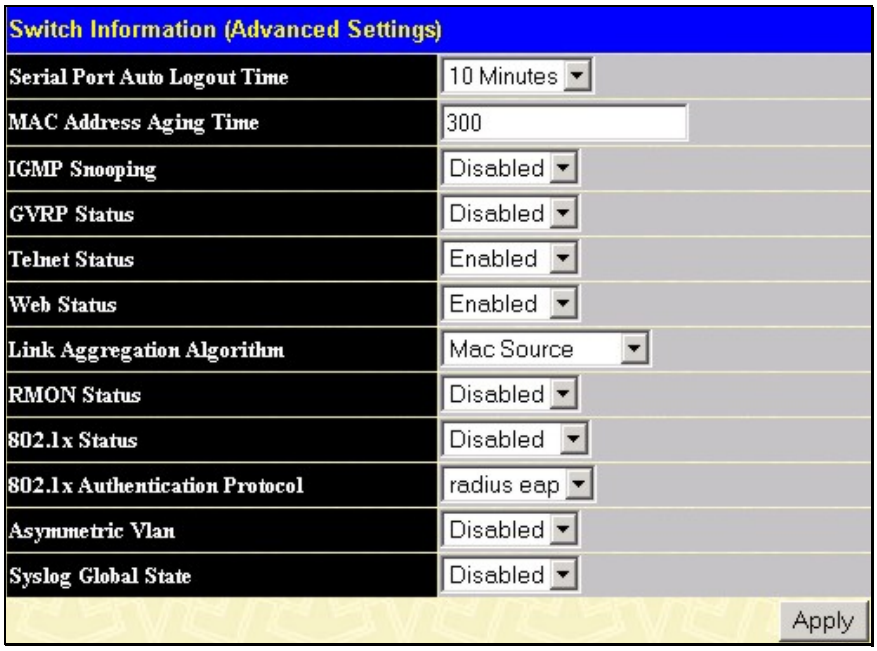



**Figure 6- 3. Switch Information (Advanced Settings)**

| Parameter | Description |
|---|---|
| **Serial Port Auto Logout Time** | Select the logout time used for the console interface. This automatically logs the user out after an idle period of time, as defined. Choose from the following options: *2 Minutes, 5 Minutes, 10 Minutes, 15 Minutes,* or *Never.* The default setting is 10 minutes. |
| **MAC Address Aging Time** | This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The default age-out time for the Switch is 300 seconds. To change this, type in a different value representing the MAC address age-out time in seconds. The Aging Time can be set to any value between **10** and **1,000,000** seconds. The default setting is 300 seconds. |
| **IGMP Snooping** | To enable system-wide IGMP Snooping capability select *Enabled*. IGMP snooping is *Disabled* by default. Enabling IGMP snooping allows you to specify use of a multicast router only (see below). To configure IGMP Snooping for individual VLANs, use the **IGMP Snooping** page under the **IGMP** folder. |
| **GVRP Status** | Use this pull-down menu to *Enable* or *Disable* GVRP on the Switch. |
| **Telnet Status** | Telnet configuration is *Enabled* by default. If you do not want to allow configuration of the system through Telnet choose *Disabled*. |
| **Web Status** | Web-based management is *Enabled* by default. If you choose to disable this by selecting *Disabled*, you will lose the ability to configure the system through the Web interface as soon as these settings are applied. |
| **Link Aggregation Algorithm** | The algorithm that the Switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose *MAC Source, MAC Destination, MAC Src & Dest, IP Source, IP Destination,* or *IP Src & Dest* (See the Link Aggregation section of this manual). |

| | |
|---|---|
| **RMON Status** | Remote monitoring (RMON) of the Switch is *Enabled* or *Disabled* here. |
| **802.1x Status** | Enables or disables 802.1x; default is *Disabled*. |
| **802.1x Authentication Protocol** | The user may use the pull down menu to choose between *Radius Eap* and *Radius Pap* for the 802.1x authentication protocol on the Switch. The default setting is *Radius Eap.* |
| **Asymmetric Vlan** | This field will enable or disable Asymmetric VLANs on the Switch. The default is *Disabled*. |
| **Syslog Global State** | Enables or disables Syslog State; default is *Disabled*. |

Click *Apply* to implement changes made to this window.

**NOTE:** When the Asymmetric VLAN function is Disabled, the user must change the VLAN setting on the Switch to its default configurations.

## Port Configurations

This section contains information for configuring various attributes and properties for individual physical ports, including port speed and flow control. Clicking on **Port Configurations** in the **Configuration** menu will display the following window for the user:

**Port Configuration**

| From | To | State | Speed/Duplex | FlowCtrl | Learn | Apply |
|---|---|---|---|---|---|---|
| Port 1 | Port 1 | Disabled | Auto | Disabled | Disabled | Apply |

**The Port Information Table**

| Port | State | Speed/Duplex | Connection | FlowCtrl | Learn |
|---|---|---|---|---|---|
| 1 | Enabled | Auto | 100M/Full/None | Disabled | Enabled |
| 2 | Enabled | Auto | Link Down | Disabled | Enabled |
| 3 | Enabled | Auto | Link Down | Disabled | Enabled |
| 4 | Enabled | Auto | Link Down | Disabled | Enabled |
| 5 | Enabled | Auto | Link Down | Disabled | Enabled |
| 6 | Enabled | Auto | Link Down | Disabled | Enabled |
| 7 | Enabled | Auto | Link Down | Disabled | Enabled |
| 8 | Enabled | Auto | Link Down | Disabled | Enabled |
| 9 | Enabled | Auto | Link Down | Disabled | Enabled |
| 10 | Enabled | Auto | Link Down | Disabled | Enabled |
| 11 | Enabled | Auto | Link Down | Disabled | Enabled |
| 12 | Enabled | Auto | Link Down | Disabled | Enabled |
| 13 | Enabled | Auto | Link Down | Disabled | Enabled |
| 14 | Enabled | Auto | Link Down | Disabled | Enabled |
| 15 | Enabled | Auto | Link Down | Disabled | Enabled |
| 16 | Enabled | Auto | Link Down | Disabled | Enabled |
| 17 | Enabled | Auto | Link Down | Disabled | Enabled |
| 18 | Enabled | Auto | Link Down | Disabled | Enabled |
| 19 | Enabled | Auto | Link Down | Disabled | Enabled |
| 20 | Enabled | Auto | Link Down | Disabled | Enabled |
| 21 | Enabled | Auto | Link Down | Disabled | Enabled |
| 22 | Enabled | Auto | Link Down | Disabled | Enabled |
| 23 | Enabled | Auto | Link Down | Disabled | Enabled |
| 24 | Enabled | Auto | Link Down | Disabled | Enabled |
| 25 | Enabled | Auto | Link Down | Disabled | Enabled |
| 26 | Enabled | Auto | Link Down | Disabled | Enabled |
| 27 | Enabled | Auto | Link Down | Disabled | Enabled |
| 28 | Enabled | Auto | Link Down | Disabled | Enabled |
| 29 | Enabled | Auto | Link Down | Disabled | Enabled |
| 30 | Enabled | Auto | Link Down | Disabled | Enabled |
| 31 | Enabled | Auto | Link Down | Disabled | Enabled |
| 32 | Enabled | Auto | Link Down | Disabled | Enabled |
| 33 | Enabled | Auto | Link Down | Disabled | Enabled |
| 34 | Enabled | Auto | Link Down | Disabled | Enabled |
| 35 | Enabled | Auto | Link Down | Disabled | Enabled |
| 36 | Enabled | Auto | Link Down | Disabled | Enabled |
| 37 | Enabled | Auto | Link Down | Disabled | Enabled |
| 38 | Enabled | Auto | Link Down | Disabled | Enabled |
| 39 | Enabled | Auto | Link Down | Disabled | Enabled |
| 40 | Enabled | Auto | Link Down | Disabled | Enabled |
| 41 | Enabled | Auto | Link Down | Disabled | Enabled |
| 42 | Enabled | Auto | Link Down | Disabled | Enabled |
| 43 | Enabled | Auto | Link Down | Disabled | Enabled |
| 44 | Enabled | Auto | Link Down | Disabled | Enabled |
| 45 | Enabled | Auto | Link Down | Disabled | Enabled |
| 46 | Enabled | Auto | Link Down | Disabled | Enabled |
| 47 | Enabled | Auto | Link Down | Disabled | Enabled |
| 48 | Enabled | Auto | Link Down | Disabled | Enabled |
| 49 | Enabled | Auto | Link Down | Disabled | Enabled |
| 50 | Enabled | Auto | Link Down | Disabled | Enabled |

**Figure 6- 4. Port Configuration and The Port Information Table window**

***To configure switch ports:***

1. Choose the port or sequential range of ports using the **From…To…** port pull-down menus.
2. Use the remaining pull-down menus to configure the parameters described below:

| Parameter | Description |
|---|---|
| **State** <*Enabled*> | Toggle the **State <***Enabled***>** field to either enable or disable a given port or group of ports. |
| **Speed/Duplex** <*Auto*> | Toggle the **Speed/Duplex <***Auto***>** field to either select the speed and duplex/half-duplex state of the port. Auto – auto-negotiation between 10 and 1000 Mbps devices, full- or half-duplex. The Auto setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *Auto, 10M/Half, 10M/Full, 100M/Half,* and *100M/Full.* There is no automatic adjustment of port settings with any option other than *Auto*. |
| **Flow Control** | Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and Auto ports use an automatic selection of the two. The default is **Disabled**. |
| **Learn** | Enable or disable MAC address learning for the selected ports. When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. When learning is *Disabled*, MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency. See the section on **Forwarding/Filtering** for information on entering MAC addresses into the forwarding table. The default setting is *Disabled*. |

Click *Apply* to implement the new settings on the Switch.

# Port Mirroring

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes. To view the **Port Mirroring** window, click **Port Mirroring** in the **Configuration** folder.

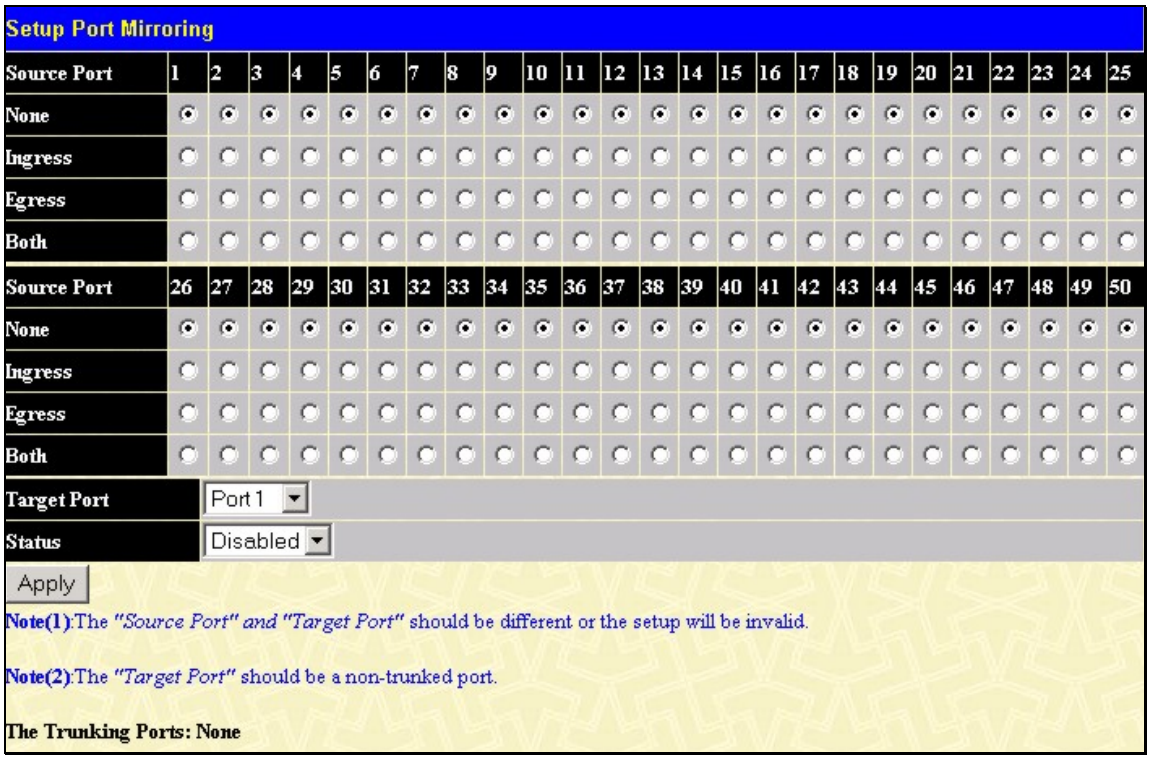

Setup Port Mirroring
Source Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
None
Ingress
Egress
Both
Source Port 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
None
Ingress
Egress
Both
Target Port
Port 1
Status
Disabled
Apply
Note(1):The "Source Port" and "Target Port" should be different or the setup will be invalid.
Note(2):The "Target Port" should be a non-trunked port.
The Trunking Ports: None

**Figure 6- 5. Setup Port Mirroring window**

***To configure a mirror port:***

1. Select the **Source Port** from where you want to copy frames and the **Target Port**, which receives the copies from the source port.
2. Select the Source Direction, **Ingress, Egress**, or **Both** and change the **Status** drop-down menu to **Enabled.**
3. Click *Apply* to make the changes take effect.

**NOTE:** You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. In addition, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port cannot be the same port.

## Port Description

The DES-3550 supports a port description feature where the user may name various ports on the Switch. To assign names to various ports, click the **Port Description** on the **Configuration** menu:

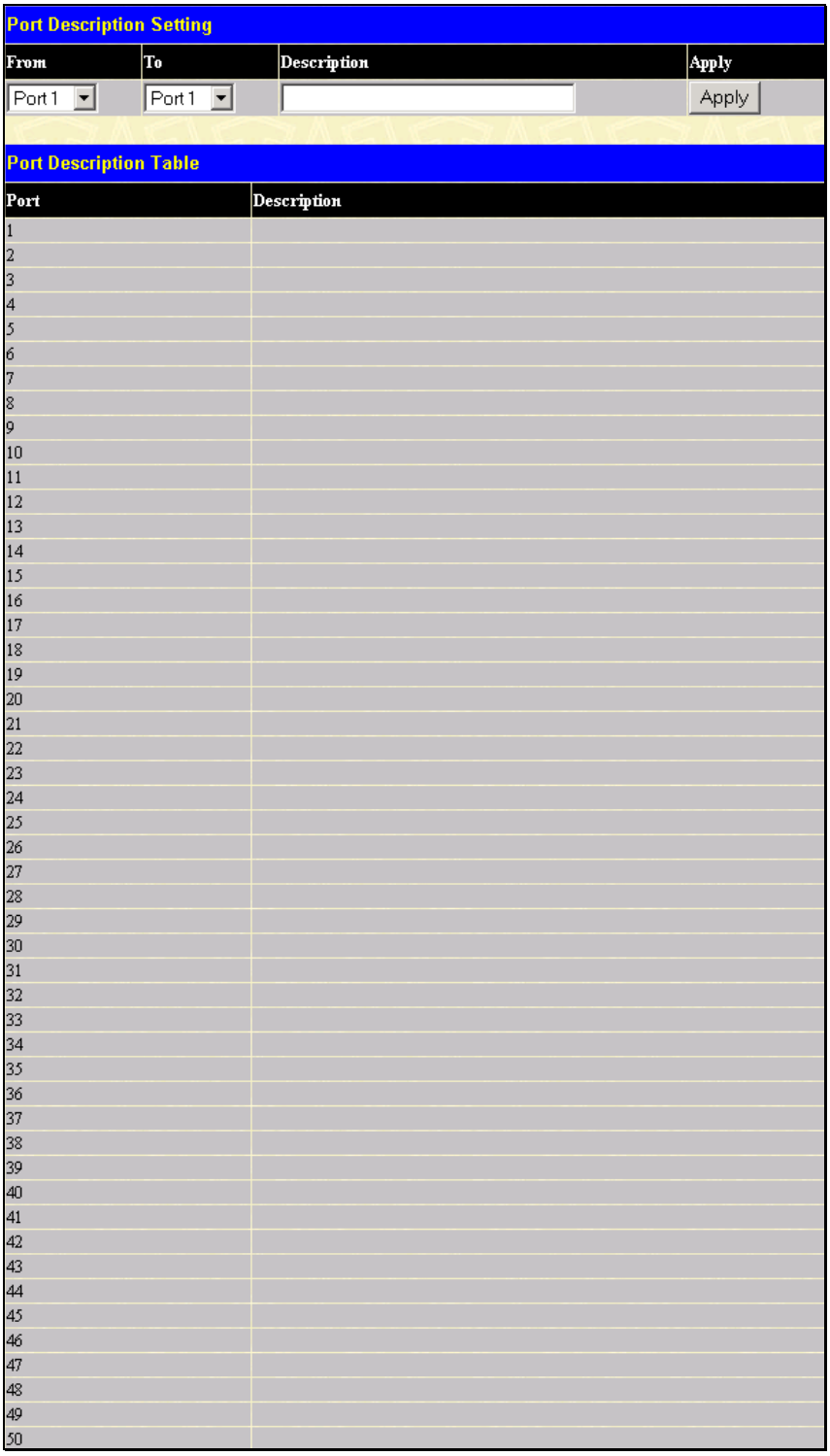



**Figure 6- 6. Port Description Setting and Port Description Table**

Use the **From** and **To** pull down menu to choose a port or range of ports to describe, and then enter a description of the port(s). Click *Apply* to set the descriptions in the **Port Description Table**.

# IGMP

**Internet Group Management Protocol (IGMP)** snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.
In order to use IGMP Snooping it must first be enabled for the entire Switch (see **Advanced Settings**). You may then fine-tune the settings for each VLAN using the **IGMP Snooping** link in the **Configuration** folder. When enabled for IGMP snooping, the Switch can open or close a port to a specific Multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

## IGMP Snooping

Use the **Current IGMP Snooping Group Entries** window to view IGMP Snooping settings. To modify the settings, click the *Modify* button of the VLAN ID you want to change.

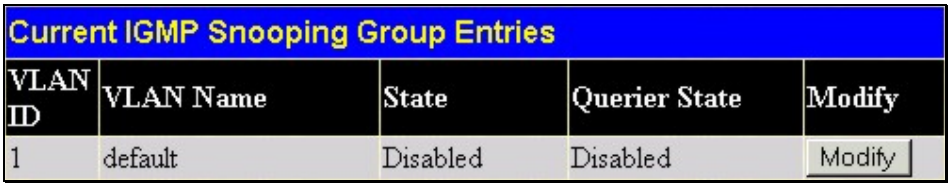



**Figure 6- 7. Current IGMP Snooping Group Entries**

Clicking the *Modify* button will bring up the **IGMP Snooping Settings** menu.

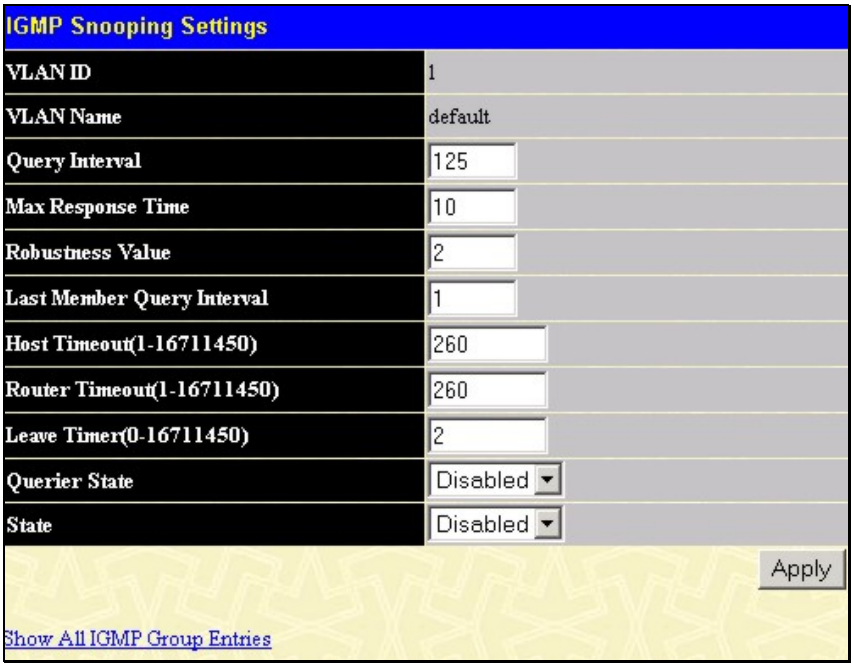



**Figure 6- 8. IGMP Snooping Settings window**

The following parameters may be viewed or modified:

| Parameter | Description |
|---|---|
| **VLAN ID** | This is the **VLAN ID** that, along with the VLAN name, identifies the VLAN that the user wishes to modify the IGMP Snooping Settings for. |
| **VLAN Name** | This is the **VLAN Name** that, along with the VLAN ID, identifies the VLAN that the user wishes to modify the IGMP Snooping Settings for. |
| **Query Interval** | The **Query Interval** field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 65535 seconds are allowed. Default = 125. |
| **Max Response Time** | This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The **Max Response Time** field allows an entry between 1 and 25 (seconds). Default = 10. |
| **Robustness Variable** | Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the **Robustness Variable** should be increased to accommodate increased packet loss. This entry field allows an entry of 1 to 255. Default = 2. |
| **Last Member Query Interval** | Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. Default = 1. |
| **Host Timeout** | This is the maximum amount of time in seconds allowed for a host to continue membership in a multicast group without the Switch receiving a host membership report. Default = 260. |
| **Route Timeout** | This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. Default = 260. |
| **Leave Timer** | This specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the **Leave Timer** expires, the (multicast) forwarding entry for that host is deleted. |
| **Querier State** | Choose *Enabled* to enable transmitting IGMP Query packets or *Disabled* to disable. The default value is *Disabled*. |
| **State** | Select *Enabled* to implement IGMP Snooping. This field is *Disabled* by default. |

Click *Apply* to implement the new settings. Click the Show All IGMP Group Entries link to return to the **Current IGMP Snooping Group Entries** window.

## Static Router Ports

A static router port is a port that has a multicast router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port will allow multicast packets coming from the router to be propagated through the network, as well as allowing multicast messages (IGMP) coming from the network to be propagated to the router. A router port has the following behavior:

- All IGMP Report packets will be forwarded to the router port.
- IGMP queries (from the router port) will be flooded to all ports.
- All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multicast router connected to the router port of the Layer 3 switch would not be able to receive UDP data streams unless the UDP multicast packets were all forwarded to the router port.

A router port will be dynamically configured when IGMP query packets, RIPv2 multicast, DVMRP multicast, or PIM-DM multicast packets are detected flowing into a port.

Open the **IGMP** folder and the click on the **Static Router Ports Entry** link to open the **Current Static Router Ports Entries** page, as shown below.

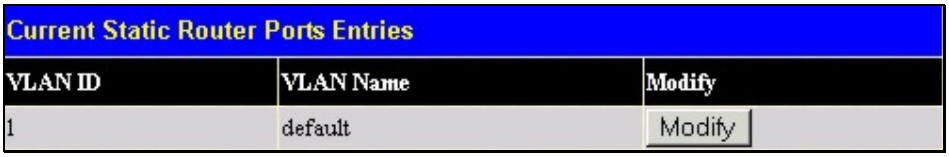



**Figure 6- 9. Current Static Router Ports Entries window**

The **Current Static Router Ports Entries** page (shown above) displays all of the current entries to the Switch's static router port table. To add or modify an entry, click the *Modify* button. This will open the **Static Router Ports Settings** page, as shown below.

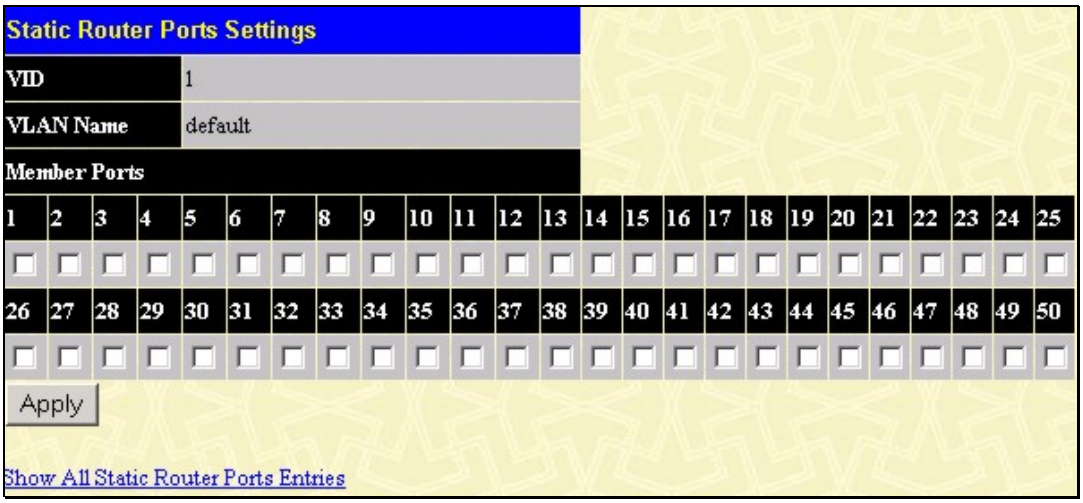



**Figure 6- 10. Static Router Ports Settings window**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **VID (VLAN ID)** | This is the VLAN ID that, along with the VLAN name, identifies the VLAN where the multicast router is attached. |
| **VLAN Name** | This is the name of the VLAN where the multicast router is attached. |
| **Member Ports** | These are the ports on the Switch that will have a multicast router attached to them. |

Click *Apply* to implement the new settings. Click the Show All Static Router Port Entries link to return to the **Current Static Router Port Entries** window.

# Spanning Tree

The Switch supports 802.1d Spanning Tree Protocol (STP) and 802.1w Rapid Spanning Tree Protocol (RSTP). 802.1d STP will be familiar to most networking professionals. However since 802.1w RSTP has been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1 d STP and 802.1w RSTP.

## 802.1w Rapid Spanning Tree

The Switch implements two versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w specification and a version compatible with the IEEE 802.1d STP. RSTP can operate with legacy equipment implementing IEEE 802.1d, however the advantages of using RSTP will be lost.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1d STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

### Port Transition States

An essential difference between the two protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. RSTP combines the transition states disabled, blocking, and listening used in 802.1d and creates a single state *Discarding*. In either case, ports do not forward packets; in the STP port transition states disabled, blocking, or listening or in the RSTP port state discarding there is no functional difference. The port is not active in the network topology. Table 5-7 below compares how the two protocols differ regarding the port state transition.

Both protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently, with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1d is this absence of immediate feedback from adjacent bridges.

| 802.1d STP | 802.1w RSTP | Forwarding? | Learning? |
|---|---|---|---|
| Disabled | Discarding | No | No |
| Blocking | Discarding | No | No |
| Listening | Discarding | No | No |
| Learning | Learning | No | Yes |
| Forwarding | Forwarding | Yes | Yes |

**Table 6- 1. Comparing Port States**

RSTP is capable of more rapid transition to a forwarding state; it no longer relies on timer configurations. RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

**Edge Port**

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

**P2P Port**

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

### 802.1d/802.1w Compatibility

RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1d format when necessary. However, any segment using 802.1 STP will not benefit from the rapid transition and rapid topology change detection of RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP.

## STP Switch Settings

The Spanning Tree Protocol (STP) operates on two levels. On the switch level, the settings are globally implemented. On the port level, the settings are implemented on a per user-defined group of ports basis. To open the following window, open the **Spanning Tree** folder in the **Configuration** menu and click the **STP Switch Settings** link.

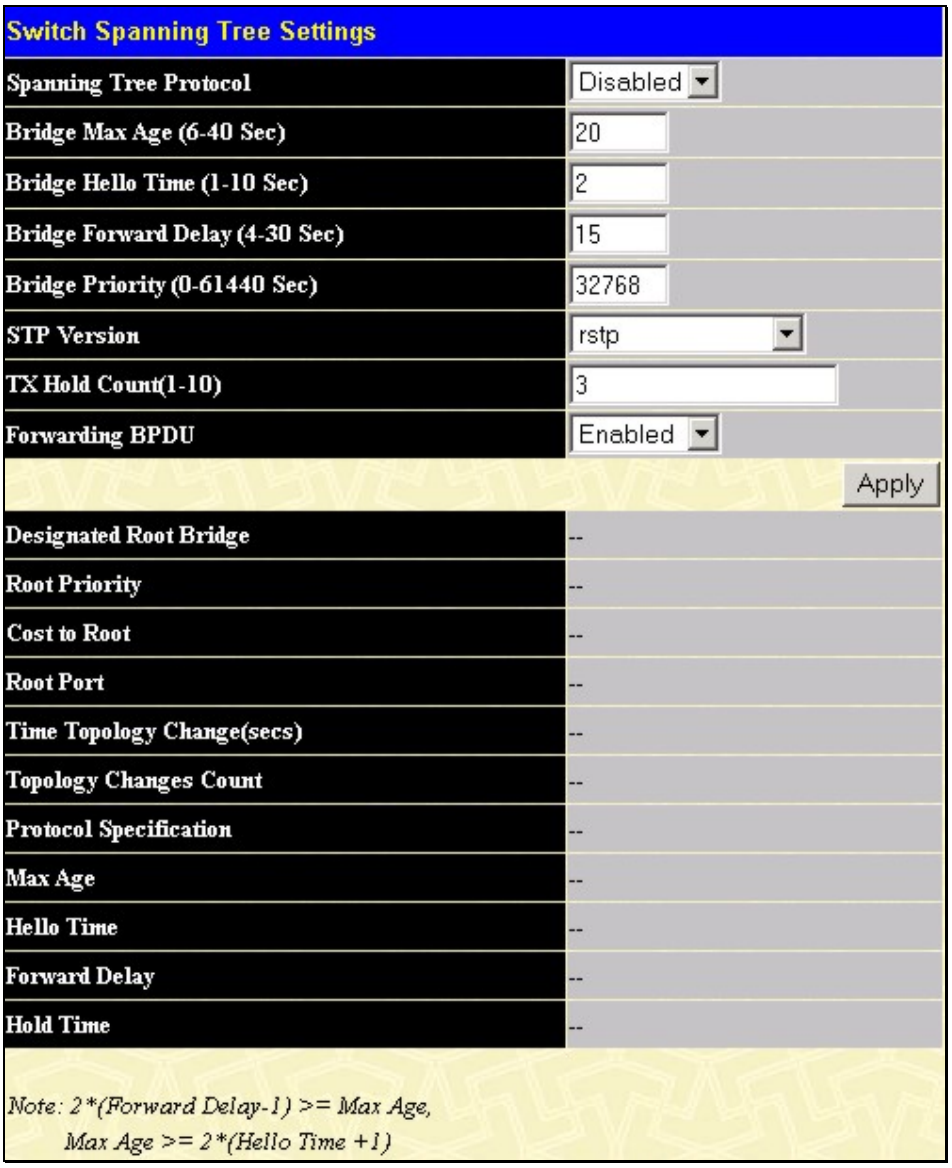



**Figure 6- 11. STP Switch Settings**

Configure the following parameters and click the *Apply* button to implement them:

| Parameter | Description |
|---|---|
| **Spanning Tree Protocol** <*Disabled*> | This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. This will enable or disable the Spanning Tree Protocol (STP), globally, for the Switch. |
| **Bridge Max Age: (6 - 40 sec)** <*20* > | The **Max. Age** can be set from 6 to 40 seconds. At the end of the Max. Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge. |
| **Bridge Hello Time: (1 - 10 sec)** < *2* > | The Hello Time can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. |

| | |
|---|---|
| **Bridge Forward Delay: (4 - 30 sec)** *<15 >* | The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state. |
| **Bridge Priority: (0 - 61440)** *<32768>* | A Priority for the Switch can be set from 0 to 61440. This number is used in the voting process between switches on the network to determine which switch will be the root switch. A low number indicates a high priority, and a high probability that this switch will be elected as the root switch. |
| **STP Version***<RSTP >* | Choose RSTP (default) or STP Compatibility. Both versions use STP parameters in the same way. RSTP is fully compatible with IEEE 802.1d STP and will function with legacy equipment. |
| **Tx Hold Count** *<3 >* | This is the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. Default value = 3. |
| **Forwarding BPDU** *<Enabled >* | This field can be enabled or disabled. When it is enabled, it allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is enabled. |

Click *Apply* to implement the changes made.

**Note**: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

**Observe the following formulas when setting the above parameters:**

Max. Age ≤ 2 x (Forward Delay - 1 second)

Max. Age ≥ 2 x (Hello Time + 1 second)

## STP Port Settings

To view the STP Port Settings window, click its link in the **Configuration** folder, displaying the following screen:

**STP Port Settings**

| From | To | State | Cost | Priority | Migration | Edge | P2P | Apply |
|---|---|---|---|---|---|---|---|---|
| Port 1 | Port 1 | Disabled | 200000 | 128 | No | No | No | Apply |

**The STP Port Information**

| Port | Designated Bridge | State | Cost | Priority | Edge | P2P | STP Status | Role |
|---|---|---|---|---|---|---|---|---|
| 1 | N/A | Yes | *200000 | 128 | No | Yes | Forwarding | NonStp |
| 2 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 3 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 4 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 5 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 6 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 7 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 8 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 9 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 10 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 11 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 12 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 13 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 14 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 15 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 16 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 17 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 18 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 19 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 20 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 21 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 22 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 23 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 24 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 25 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 26 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 27 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 28 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 29 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 30 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 31 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 32 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 33 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 34 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 35 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 36 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 37 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 38 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 39 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 40 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 41 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 42 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 43 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 44 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 45 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 46 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 47 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 48 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 49 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |
| 50 | N/A | Yes | *200000 | 128 | No | Yes | Disabled | Disabled |

**Figure 6- 12. STP Port Settings and The STP Port Information window**

In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP Group will use the switch-level parameters entered above, with the addition of **Port Priority** and **Port Cost**.
An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.
The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.
It is advisable to define an STP Group to correspond to a VLAN group of ports.
The following fields can be set:

| Parameter | Description |
|---|---|
| **From/To <** *Port 1* **>** | A consecutive group of ports may be configured starting with the selected port. |
| **State <** *Disabled* **>** | This drop-down menu allows you to **Enable** or **Disable** STP for the selected group of ports. |
| **Cost <** *0* **>** | A Port Cost can be set from *1* to *200000000*. The lower the number, the greater the probability the port will be chosen to forward packets.<br>Default port cost:<br>100Mbps port = 200000<br>Gigabit ports = 20000 |
| **Priority** <*128*> | A Port Priority can be from *0* to *240*. The lower the number, the greater the probability the port will be chosen as the Root Port. |
| **Migration** <*No*> | Select Y*es* or *No*. Choosing Yes will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (yes) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment. |
| **Edge** <*No*> | Select *Yes* or *No.* Choosing Yes designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. No indicates the port does not have edge port status. |
| **P2P** <*No*> | Select *Yes* or *No*. Choosing *Yes* indicates a point-to-point (p2p) shared link. These are similar to edge ports however, they are restricted in that a p2p port must operate in full-duplex. Like edge ports, p2p ports transition to a forwarding state rapidly thus benefiting from RSTP. |

Click *Apply* to implement the changes made.

# Forwarding Filtering

## Unicast Forwarding

Open the **Forwarding Filtering** folder in the **Configuration** menu and click on the **Unicast Forwarding** link. This will open the **Setup Static Unicast Forwarding Table**, as shown below:

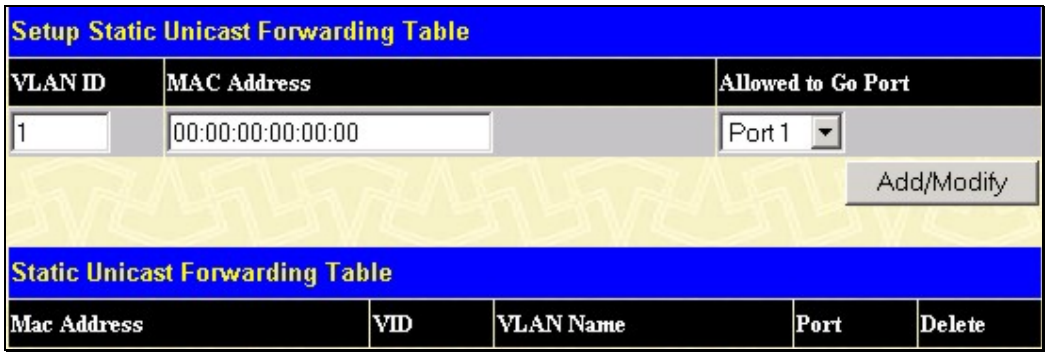



**Figure 6- 13. Setup Static Unicast Forwarding Table and Static Unicast Forwarding Table**

To add or edit an entry, define the following parameters and then click *Add/Modify*:

| Parameter | Description |
|---|---|
| **VLAN ID (VID)** | The VLAN ID number of the VLAN on which the above Unicast MAC address resides. |
| **MAC Address** | The MAC address to which packets will be statically forwarded. This must be a unicast MAC address. |
| **Allowed to Go Port** | Allows the selection of the port number on which the MAC address entered above resides. |

Click *Apply* to implement the changes made. To delete an entry in the **Static Unicast Forwarding Table**, click the corresponding ✕ under the *Delete* heading.

## Static Multicast Forwarding

The following figure and table describe how to set up Multicast forwarding on the Switch. Open the **Forwarding Filtering** folder and click on the **Multicast Forwarding** link to see the entry screen below:

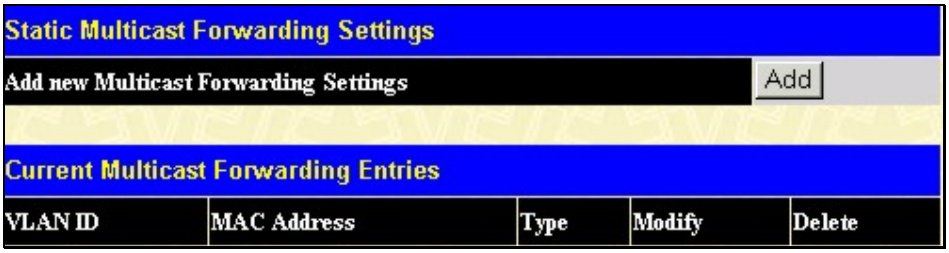



**Figure 6- 14. Static Multicast Forwarding Settings and Current Multicast Forwarding Entries**

The **Static Multicast Forwarding Settings** page displays all of the entries made into the Switch's static multicast forwarding table. Click the *Add* button to open the **Setup Static Multicast Forwarding Table**, as shown below:

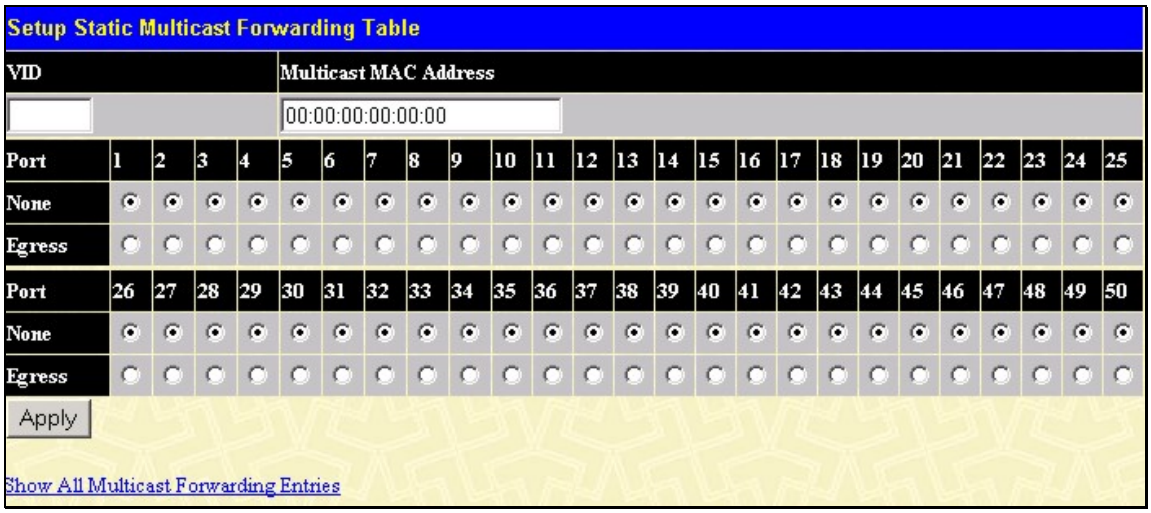

Setup Static Multicast Forwarding Table
VID
Multicast MAC Address
00:00:00:00:00:00
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
None
Egress
Port 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
None
Egress
Apply
Show All Multicast Forwarding Entries

**Figure 6- 15. Setup Static Multicast Forwarding Table**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **VID** | The VLAN ID of the VLAN the corresponding MAC address belongs to. |
| **Multicast MAC Address** | The MAC address of the static source of multicast packets. This must be a multicast MAC address. |
| **Port Settings** | Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP.<br>The options are:<br>**None** – no restrictions on the port dynamically joining the multicast group. When **None** is chosen, the port will not be a member of the Static Multicast Group.<br>**Egress** – the port is a static member of the multicast group. |

Click *Apply* to implement the changes made. To delete an entry in the **Static Multicast Forwarding Table**, click the corresponding ✕ under the *Delete* heading. Click the Show All Multicast Forwarding Entries link to return to the **Static Multicast Forwarding Settings** window.

## Multicast Port Filtering

The following figure and table describe how to set up Multicast forwarding on the Switch. Open the **Forwarding Filtering** folder and click on the **Multicast Port Filtering Mode Setup** link to see the entry screen below:

**Multicast Port Filtering Mode Setup**

| From | To | Mode | Apply |
|---|---|---|---|
| Port 1 | Port 1 | Forward All Groups | Apply |

**Multicast Port Filtering Mode Table**

| Port | Mode |
|---|---|
| 1 | Forward Unregistered Groups |
| 2 | Forward Unregistered Groups |
| 3 | Forward Unregistered Groups |
| 4 | Forward Unregistered Groups |
| 5 | Forward Unregistered Groups |
| 6 | Forward Unregistered Groups |
| 7 | Forward Unregistered Groups |
| 8 | Forward Unregistered Groups |
| 9 | Forward Unregistered Groups |
| 10 | Forward Unregistered Groups |
| 11 | Forward Unregistered Groups |
| 12 | Forward Unregistered Groups |
| 13 | Forward Unregistered Groups |
| 14 | Forward Unregistered Groups |
| 15 | Forward Unregistered Groups |
| 16 | Forward Unregistered Groups |
| 17 | Forward Unregistered Groups |
| 18 | Forward Unregistered Groups |
| 19 | Forward Unregistered Groups |
| 20 | Forward Unregistered Groups |
| 21 | Forward Unregistered Groups |
| 22 | Forward Unregistered Groups |
| 23 | Forward Unregistered Groups |
| 24 | Forward Unregistered Groups |
| 25 | Forward Unregistered Groups |
| 26 | Forward Unregistered Groups |
| 27 | Forward Unregistered Groups |
| 28 | Forward Unregistered Groups |
| 29 | Forward Unregistered Groups |
| 30 | Forward Unregistered Groups |
| 31 | Forward Unregistered Groups |
| 32 | Forward Unregistered Groups |
| 33 | Forward Unregistered Groups |
| 34 | Forward Unregistered Groups |
| 35 | Forward Unregistered Groups |
| 36 | Forward Unregistered Groups |
| 37 | Forward Unregistered Groups |
| 38 | Forward Unregistered Groups |
| 39 | Forward Unregistered Groups |
| 40 | Forward Unregistered Groups |
| 41 | Forward Unregistered Groups |
| 42 | Forward Unregistered Groups |
| 43 | Forward Unregistered Groups |
| 44 | Forward Unregistered Groups |
| 45 | Forward Unregistered Groups |
| 46 | Forward Unregistered Groups |
| 47 | Forward Unregistered Groups |
| 48 | Forward Unregistered Groups |
| 49 | Forward Unregistered Groups |
| 50 | Forward Unregistered Groups |

**Figure 6- 16. Multicast Port Filtering Mode Setup and Multicast port Filtering Mode Table**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **From/To** | These two drop-down menus allow you to select a range of ports that the filter settings will be applied to. |
| **Mode** | This drop-down menu allows you to select the action the Switch will take when it receives a multicast packet that is to be forwarded to one of the ports in the range specified above.<br>**Forward All Groups –** instructs the Switch to forward a multicast packet to all multicast groups residing within the range of ports specified above.<br>**Forward Unregistered Groups –** instructs the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above.<br>**Filter Unregistered Groups –** instructs the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above. |

Click *Apply* to implement the changes made.

# VLANs

## Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users, whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, it is recommended that the highest priority queue, Queue 1, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

A weighted round robin system is employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 1, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

## VLANs

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

### Notes About VLANs on the DES-3550

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets **cannot** cross VLANs without a network device performing a routing function between the VLANs.
The DES-3550 supports IEEE 802.1Q VLANs and Port-Based VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.
The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."
The "default" VLAN has a VID = 1.
The member ports of Port-based VLANs may overlap, if desired.

## IEEE 802.1Q VLANs

**Some relevant terms**:

**Tagging** – The act of putting 802.1Q VLAN information into the header of a packet.

**Untagging** – The act of stripping 802.1Q VLAN information out of the packet header.

**Ingress port** – A port on a switch where packets are flowing into the switch and VLAN decisions must be made.

**Egress port** – A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the Switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast, and unicast packets from unknown sources.

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

Any port can be configured as either *tagging* or *untagging*. The *untagging* feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that do not recognize VLAN tags in packet headers. The *tagging* feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN the receiving port is a member of.

The main characteristics of IEEE 802.1Q are as follows:

Assigns packets to VLANs by filtering.
Assumes the presence of a single global spanning tree.
Uses an explicit tagging scheme with one-level tagging.

### 802.1Q VLAN Packet Forwarding

Packet forwarding decisions are made based upon the following three types of rules:

Ingress rules – rules relevant to the classification of received frames belonging to a VLAN.
Forwarding rules between ports – decides whether to filter or forward the packet.
Egress rules – determines if the packet must be sent tagged or untagged.

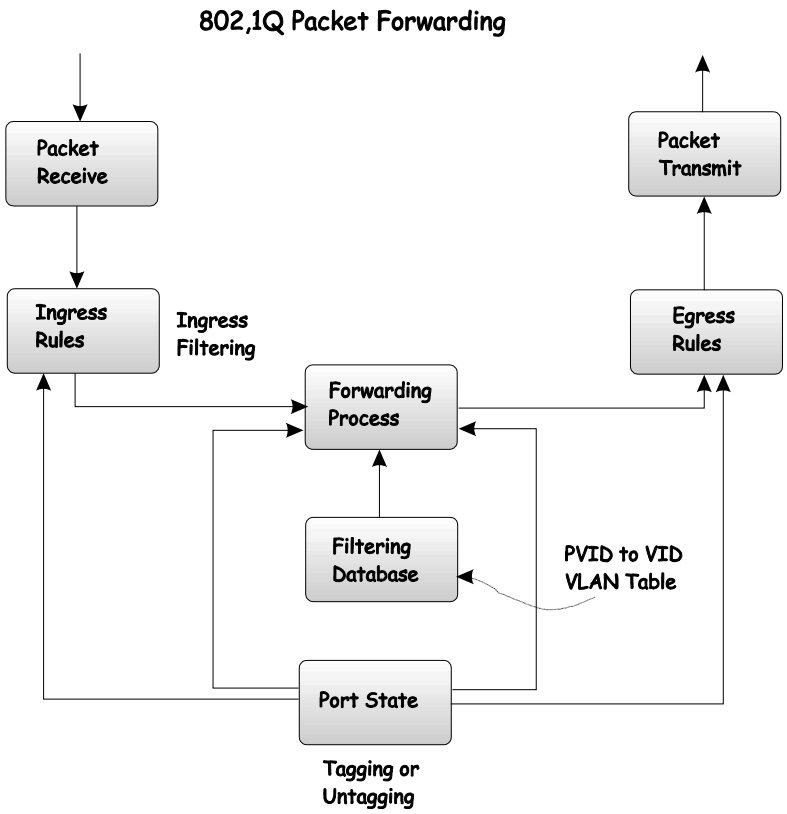



**Figure 6- 17. IEEE 802.1Q Packet Forwarding**

## 802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI – used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

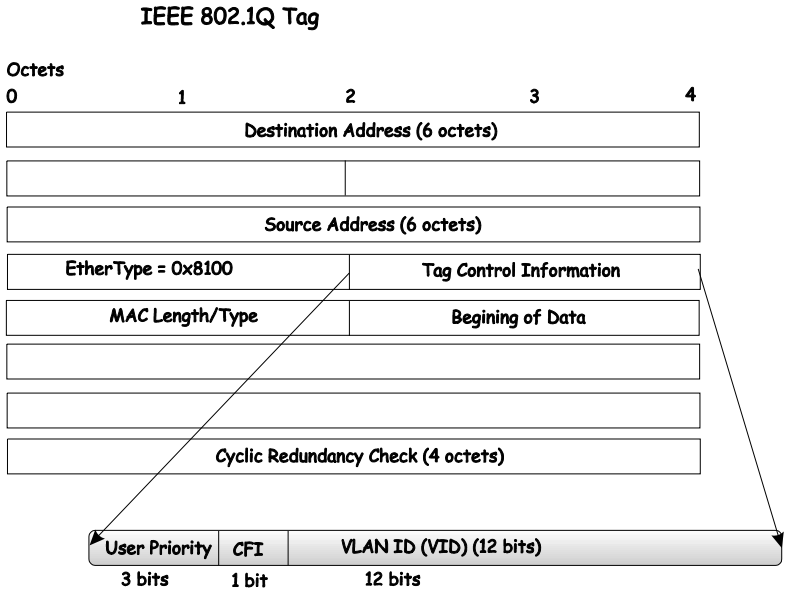



**Figure 6- 18. IEEE 802.1Q Tag**

The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

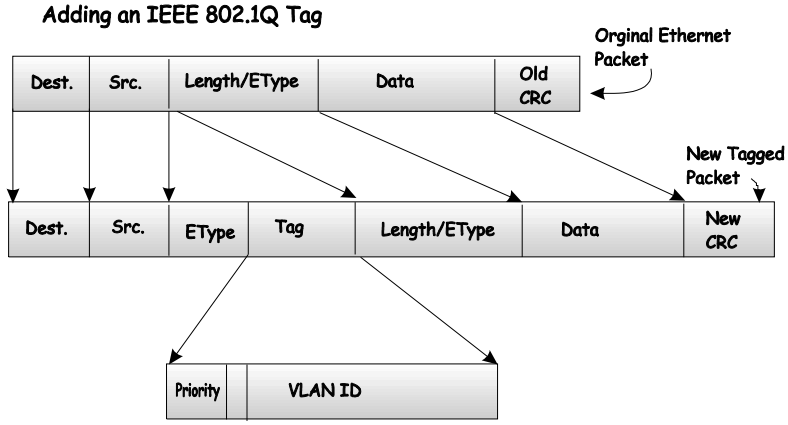



**Figure 6- 19. Adding an IEEE 802.1Q Tag**

## Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as *tag-unaware.* 802.1Q devices are referred to as *tag-aware.*

Prior to the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address (found in the Switch's

forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet.

Within the Switch, different PVIDs mean different VLANs (remember that two VLANs cannot communicate without an external router). Therefore, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, as far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the Switch to VIDs on the network. The Switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the Switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the Switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

### Tagging and Untagging

Every port on an 802.1Q compliant switch can be configured as *tagging* or *untagging*.

Ports with tagging enabled will put the VID number, priority, and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet does not have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch.) Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

### Ingress Filtering

A port on a switch where packets are flowing into the switch and VLAN decisions must be made is referred to as an *ingress port*. If ingress filtering is enabled for a port, the switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as *ingress filtering* and is used to conserve bandwidth within the Switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

### Default VLANs

The Switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in Port-based mode, their respective member ports are removed from the "default."

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

**Note**: If no VLANs are configured on the Switch, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

An example is presented below:

| VLAN Name | VID | Switch Ports |
|---|---|---|
| System (default) | 1 | 5, 6, 7, 8, 21, 22, 23, 24 |
| Engineering | 2 | 9, 10, 11, 12 |
| Marketing | 3 | 13, 14, 15, 16 |
| Finance | 4 | 17, 18, 19, 20 |
| Sales | 5 | 1, 2, 3, 4 |

**Table 6-1. VLAN Example – Assigned Ports**

## Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet is dropped by the Switch or delivered.

### VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

Network resources such as printers and servers however, can be shared across VLANs. This is achieved by setting up overlapping VLANs. That is, ports can belong to more than one VLAN group. For example, setting VLAN 1 members to ports 1, 2, 3, and 4 and VLAN 2 members to ports 1, 5, 6, and 7. Port 1 belongs to two VLAN groups. Ports 8, 9, and 10 are not configured to any VLAN group. This means ports 8, 9, and 10 are in the same VLAN group.

### VLAN and Trunk Groups

The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.

**Note**: In order to use VLAN segmentation in conjunction with port trunk groups, you can first set the port trunk group(s), and then you may configure VLAN settings. If you wish to change the port trunk grouping with VLANs already in place, you will not need to reconfigure the VLAN settings after changing the port trunk group settings. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

## Static VLAN Entry

In the **Configuration** folder, open the **VLAN** folder and click the **Static VLAN Entry** link to open the following window:

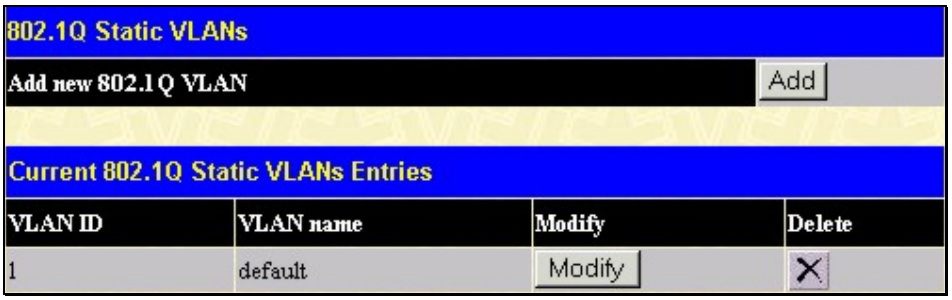



**Figure 6- 20. Current 802.1Q Static VLANs Entries window**

The 802.1Q Static VLANs menu lists all previously configured VLANs by VLAN ID and name. To delete an existing 802.1Q VLAN, click the corresponding ✕ button under the **Delete** heading.

To create a new 802.1Q VLAN, click the *Add* button in the Static VLANs menu. A new menu will appear, as shown below, to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new menu.

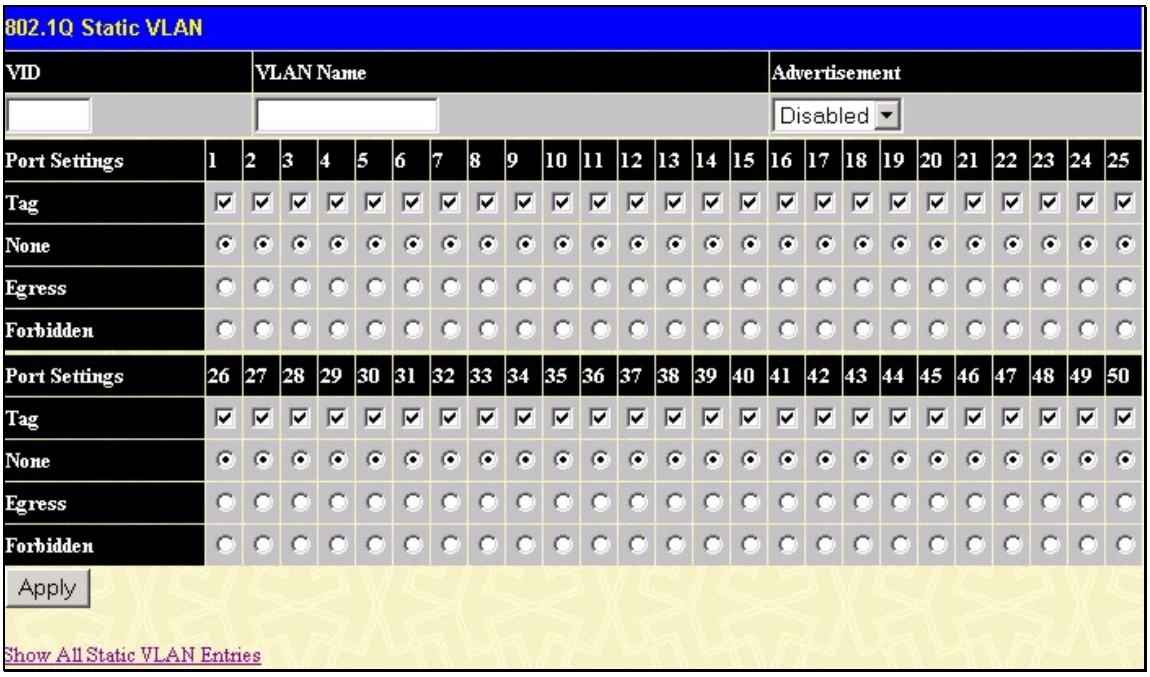

802.1Q Static VLAN
VID
VLAN Name
Advertisement
Disabled
Port Settings
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
Tag
None
Egress
Forbidden
Port Settings
26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
Tag
None
Egress
Forbidden
Apply
Show All Static VLAN Entries

**Figure 6- 21. 802.1Q Static VLANs – Add**

To return to the **Current 802.1Q Static VLANs Entries** window, click the Show All Static VLAN Entries link. To change an existing 802.1Q VLAN entry, click the *Modify* button of the corresponding entry you wish to modify. A new menu appears; use this to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new menu.

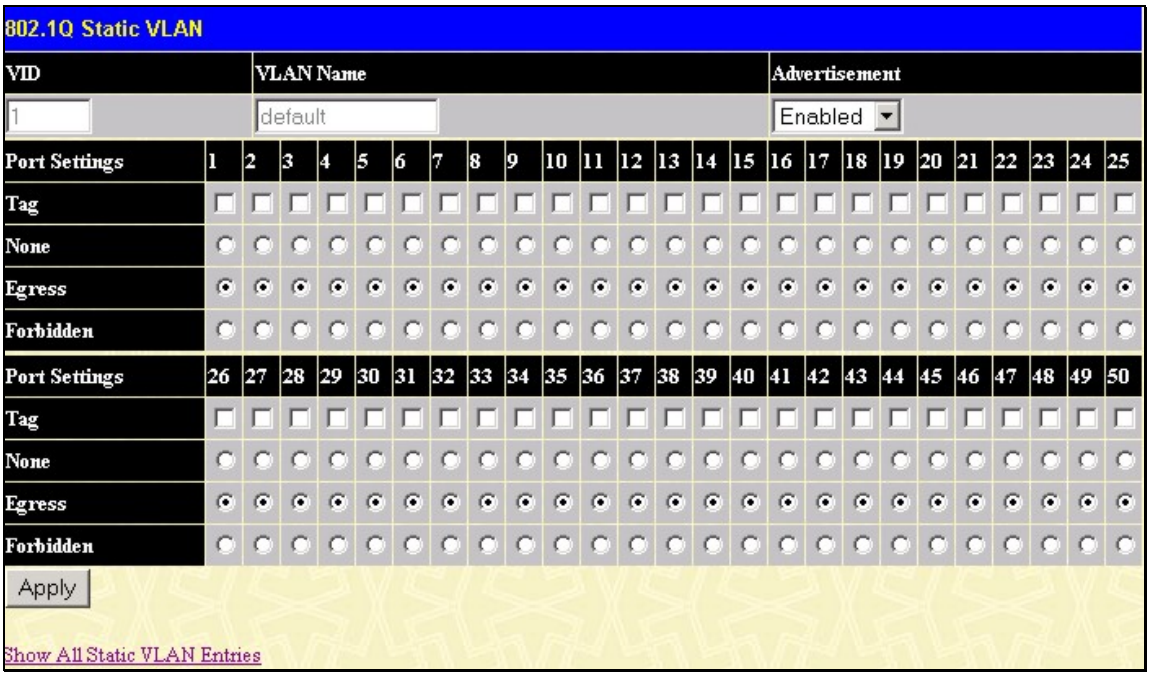

802.1Q Static VLAN
VID
VLAN Name
Advertisement
1
default
Enabled
Port Settings 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
Tag
None
Egress
Forbidden
Port Settings 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
Tag
None
Egress
Forbidden
Apply
Show All Static VLAN Entries

**Figure 6- 22. 802.1Q Static VLANs Entry Settings – Modify**

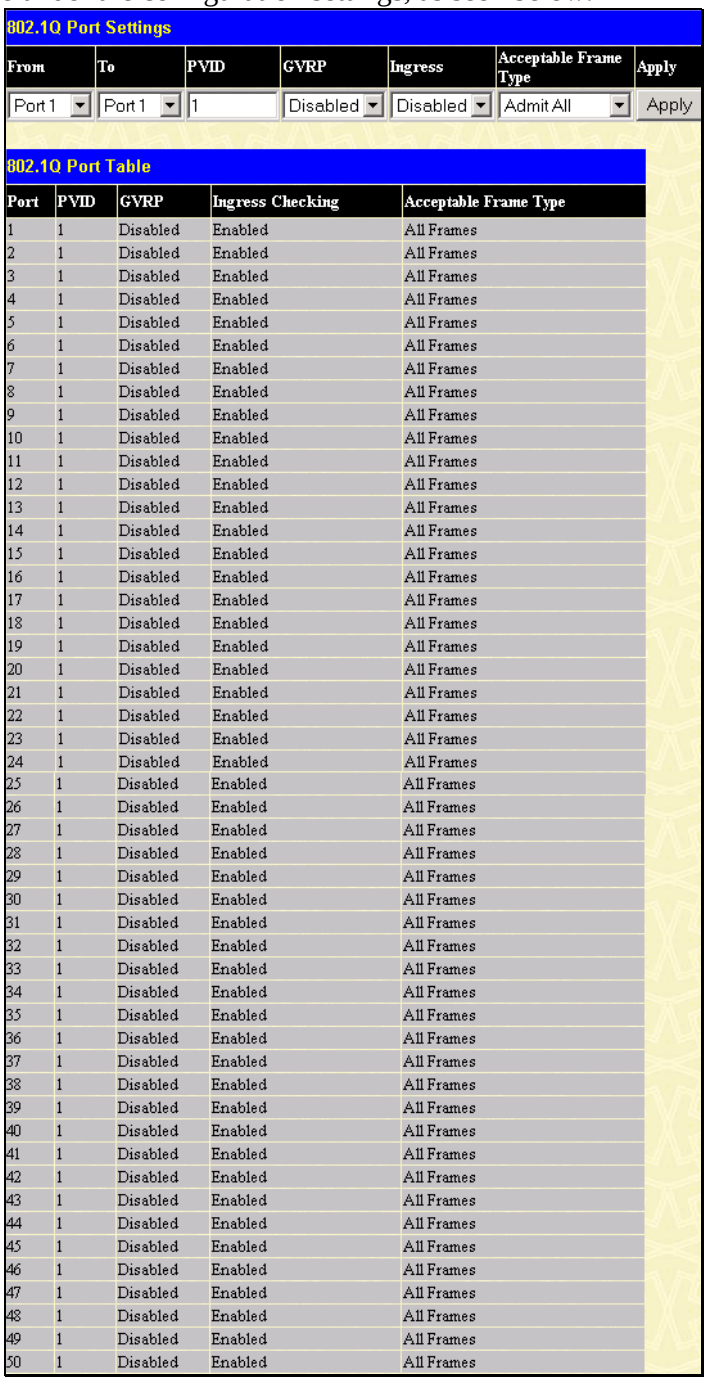
The following fields can then be set in either the *Add* or *Modify* **802.1Q Static VLANs** menus:

| Parameter | Description |
|---|---|
| **VID** (VLAN ID) | Allows the entry of a VLAN ID in the Add dialog box, or displays the VLAN ID of an existing VLAN in the Edit dialog box. VLANs can be identified by either the VID or the VLAN name. |
| **VLAN Name** | Allows the entry of a name for the new VLAN in the Add dialog box, or for editing the VLAN name in the Edit dialog box. |
| **Advertisement** | Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN. |
| **Port Settings** | Allows an individual port to be specified as member of a VLAN. |
| **Tag** | Specifies the port as either 802.1Q tagging or 802.1Q untagged. Checking the box will designate the port as Tagged. |
| **None** | Allows an individual port to be specified as a non-VLAN member. |
| **Egress** | Select this to specify the port as a static member of the VLAN. Egress member ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged. |
| **Forbidden** | Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically. |

Click *Apply* to implement changes made.

## Port VLAN ID(PVID)

In the **Configuration** menu, open the **VLANs** folder and click **Port VLAN ID**.
The **802.1Q Port Settings** dialog box, shown below, allows you to determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (**GVRP**) enabled switches. In addition, **Ingress** Checking can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.



802.1Q Port Settings

| From | To | PVID | GVRP | Ingress | Acceptable Frame Type | Apply |
|---|---|---|---|---|---|---|
| Port 1 | Port 1 | 1 | Disabled | Disabled | Admit All | Apply |

802.1Q Port Table

| Port | PVID | GVRP | Ingress Checking | Acceptable Frame Type |
|---|---|---|---|---|
| 1 | 1 | Disabled | Enabled | All Frames |
| 2 | 1 | Disabled | Enabled | All Frames |
| 3 | 1 | Disabled | Enabled | All Frames |
| 4 | 1 | Disabled | Enabled | All Frames |
| 5 | 1 | Disabled | Enabled | All Frames |
| 6 | 1 | Disabled | Enabled | All Frames |
| 7 | 1 | Disabled | Enabled | All Frames |
| 8 | 1 | Disabled | Enabled | All Frames |
| 9 | 1 | Disabled | Enabled | All Frames |
| 10 | 1 | Disabled | Enabled | All Frames |
| 11 | 1 | Disabled | Enabled | All Frames |
| 12 | 1 | Disabled | Enabled | All Frames |
| 13 | 1 | Disabled | Enabled | All Frames |
| 14 | 1 | Disabled | Enabled | All Frames |
| 15 | 1 | Disabled | Enabled | All Frames |
| 16 | 1 | Disabled | Enabled | All Frames |
| 17 | 1 | Disabled | Enabled | All Frames |
| 18 | 1 | Disabled | Enabled | All Frames |
| 19 | 1 | Disabled | Enabled | All Frames |
| 20 | 1 | Disabled | Enabled | All Frames |
| 21 | 1 | Disabled | Enabled | All Frames |
| 22 | 1 | Disabled | Enabled | All Frames |
| 23 | 1 | Disabled | Enabled | All Frames |
| 24 | 1 | Disabled | Enabled | All Frames |
| 25 | 1 | Disabled | Enabled | All Frames |
| 26 | 1 | Disabled | Enabled | All Frames |
| 27 | 1 | Disabled | Enabled | All Frames |
| 28 | 1 | Disabled | Enabled | All Frames |
| 29 | 1 | Disabled | Enabled | All Frames |
| 30 | 1 | Disabled | Enabled | All Frames |
| 31 | 1 | Disabled | Enabled | All Frames |
| 32 | 1 | Disabled | Enabled | All Frames |
| 33 | 1 | Disabled | Enabled | All Frames |
| 34 | 1 | Disabled | Enabled | All Frames |
| 35 | 1 | Disabled | Enabled | All Frames |
| 36 | 1 | Disabled | Enabled | All Frames |
| 37 | 1 | Disabled | Enabled | All Frames |
| 38 | 1 | Disabled | Enabled | All Frames |
| 39 | 1 | Disabled | Enabled | All Frames |
| 40 | 1 | Disabled | Enabled | All Frames |
| 41 | 1 | Disabled | Enabled | All Frames |
| 42 | 1 | Disabled | Enabled | All Frames |
| 43 | 1 | Disabled | Enabled | All Frames |
| 44 | 1 | Disabled | Enabled | All Frames |
| 45 | 1 | Disabled | Enabled | All Frames |
| 46 | 1 | Disabled | Enabled | All Frames |
| 47 | 1 | Disabled | Enabled | All Frames |
| 48 | 1 | Disabled | Enabled | All Frames |
| 49 | 1 | Disabled | Enabled | All Frames |
| 50 | 1 | Disabled | Enabled | All Frames |

**Figure 6- 23. 802.1Q Port Settings and 802.1Q Port Table**

The following fields can be set:

| Parameter | Description |
|---|---|
| **From/To** | These two fields allow you to specify the range of ports that will be included in the Port-based VLAN that you are creating using the **802.1Q Port Settings** page. |
| **PVID** | The read only field in the **GVRP Table** shows the current PVID assignment for each port. The Switch's default is to assign all ports to the Default VLAN with a VID of 1.<br>The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions.<br>If a packet is received by the port, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet. |
| **GVRP** | The **Group VLAN Registration Protocol (GVRP)** enables the port to dynamically become a member of a VLAN. **GVRP** is disabled by default. |
| **Ingress** | This field can be toggled using the space bar between *Enabled* and *Disabled*. *Enabled* enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. *Disabled* disables Ingress filtering. Ingress Checking is disabled by default. |
| **Acceptable Frame Type** | This field denotes the type of frame that will be accepted by the port. The user may choose between **Tagged Only,** which means only VLAN tagged frames will be accepted, and **Admit_All,** which means both tagged and untagged frames will be accepted. **Admit_All** is enabled by default. |

Click *Apply* to implement the changes made.

# Port Bandwidth

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port. In the **Configuration** folder, click **Port Bandwidth**, to view the screen shown below.

**Bandwidth Settings**

| From | To | Type | No Limit | Rate | Apply |
|---|---|---|---|---|---|
| Port 1 | Port 1 | RX | Disabled | 1 | Apply |

**Port Bandwidth Table**

| Port | RX Rate (Mbit/sec) | TX Rate (Mbit/sec) |
|---|---|---|
| 1 | No Limit | no_limit |
| 2 | No Limit | no_limit |
| 3 | No Limit | no_limit |
| 4 | No Limit | no_limit |
| 5 | No Limit | no_limit |
| 6 | No Limit | no_limit |
| 7 | No Limit | no_limit |
| 8 | No Limit | no_limit |
| 9 | No Limit | no_limit |
| 10 | No Limit | no_limit |
| 11 | No Limit | no_limit |
| 12 | No Limit | no_limit |
| 13 | No Limit | no_limit |
| 14 | No Limit | no_limit |
| 15 | No Limit | no_limit |
| 16 | No Limit | no_limit |
| 17 | No Limit | no_limit |
| 18 | No Limit | no_limit |
| 19 | No Limit | no_limit |
| 20 | No Limit | no_limit |
| 21 | No Limit | no_limit |
| 22 | No Limit | no_limit |
| 23 | No Limit | no_limit |
| 24 | No Limit | no_limit |
| 25 | No Limit | no_limit |
| 26 | No Limit | no_limit |
| 27 | No Limit | no_limit |
| 28 | No Limit | no_limit |
| 29 | No Limit | no_limit |
| 30 | No Limit | no_limit |
| 31 | No Limit | no_limit |
| 32 | No Limit | no_limit |
| 33 | No Limit | no_limit |
| 34 | No Limit | no_limit |
| 35 | No Limit | no_limit |
| 36 | No Limit | no_limit |
| 37 | No Limit | no_limit |
| 38 | No Limit | no_limit |
| 39 | No Limit | no_limit |
| 40 | No Limit | no_limit |
| 41 | No Limit | no_limit |
| 42 | No Limit | no_limit |
| 43 | No Limit | no_limit |
| 44 | No Limit | no_limit |
| 45 | No Limit | no_limit |
| 46 | No Limit | no_limit |
| 47 | No Limit | no_limit |
| 48 | No Limit | no_limit |
| 49 | No Limit | no_limit |
| 50 | No Limit | no_limit |

**Figure 6- 24. Bandwidth Settings and Port Bandwidth Table**

The following parameters can be set or are displayed:

| Parameter | Description |
|---|---|
| **From/To** | A consecutive group of ports may be configured starting with the selected port. |
| **Type** | This drop-down menu allows you to select between **RX** (receive), **TX** (transmit), and **Both**. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets. |
| **no_limit** | This drop-down menu allows you to specify that the selected port will have no bandwidth limit. **Enabled** disables the limit. |
| **Rate** | This field allows you to enter the data rate, in kb/s, that will be the limit for the selected port. |

Click *Apply* to set the Bandwidth control for the selected ports. Results of the **Bandwidth Settings** will be displayed, in the **Port Bandwidth Table.**

# SNTP Settings

## Current Time Settings

To configure the time settings for the Switch, open the **Configuration** folder, then the **SNTP** folder and click on the **Current Time Setting** link, revealing the following screen for the user to configure.

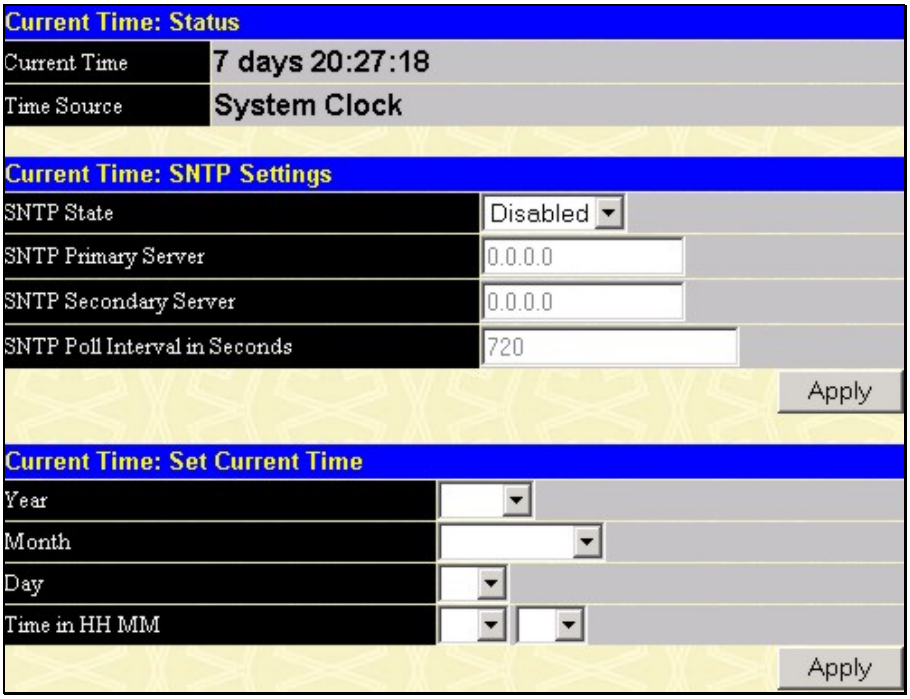



**Figure 6- 25. Time Settings Page**

The following parameters can be set or are displayed:

| Parameter | Description |
|---|---|
| **Current Time** | Displays the time when the Switch was initially started for this session. |
| **Time Source** | Displays the time source for the system. |
| **SNTP State** | Use this pull-down menu to **Enable** or **Disable** SNTP. |
| **SNTP Primary Server** | This is the IP address of the primary server the SNTP information will be taken from. |
| **SNTP Secondary Server** | This is the IP address of the secondary server the SNTP information will be taken from. |
| **SNTP Poll Interval in Seconds** | This is the interval, in seconds, between requests for updated SNTP information. |
| **Year** | Enter the current year, if you want to update the system clock. |
| **Month** | Enter the current month, if you would like to update the system clock. |
| **Day** | Enter the current day, if you would like to update the system clock. |
| **Time in HH MM** | Enter the current time in hours and minutes, if you would like to update the system clock. |

Click *Apply* to implement your changes.

## Time Zone and DST

The following are screens used to configure time zones and Daylight Savings time settings for SNTP. Open the **Configuration** folder, then the **SNTP** folder and click on the **Time Zone and DST** link, revealing the following screen.

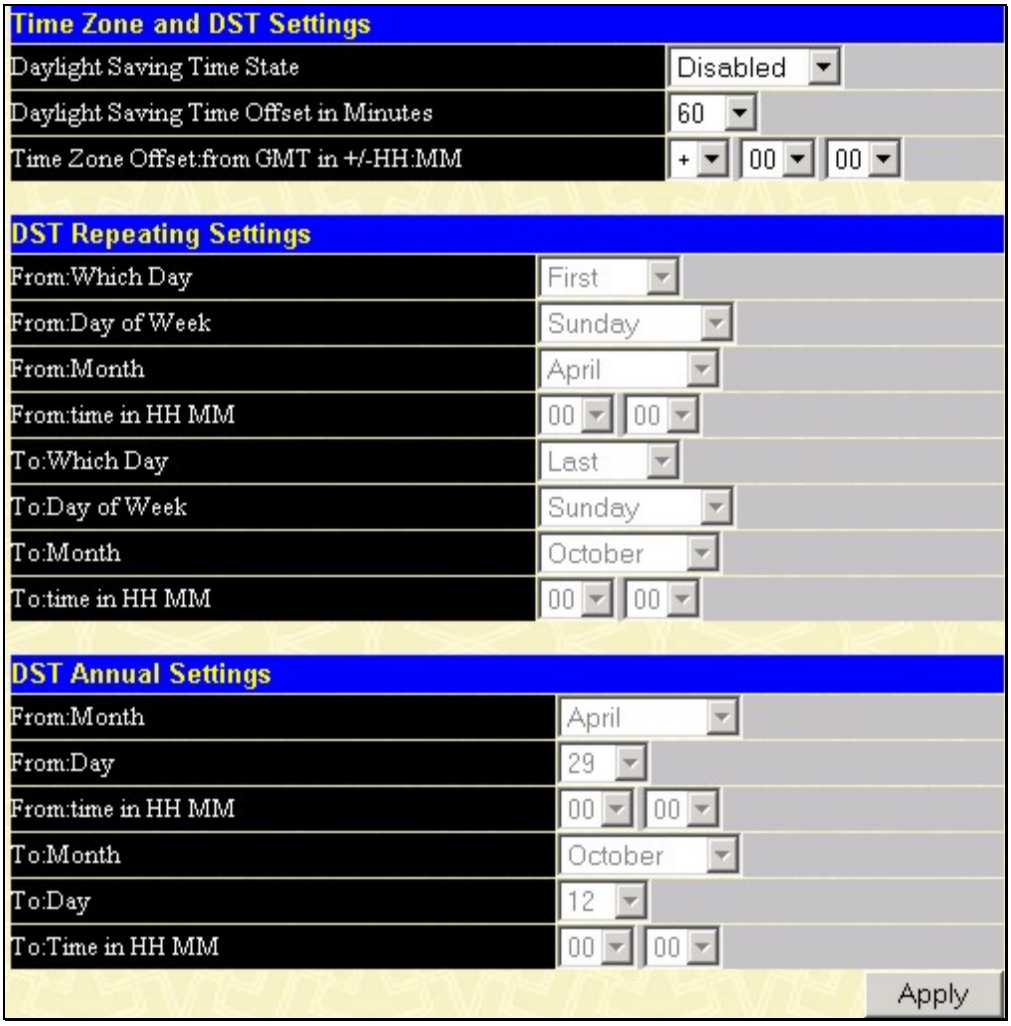



**Figure 6- 26. Time Zone and DST Settings Page**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **Daylight Saving Time State** | Use this pull-down menu to **Enable** or **Disable** the DST Settings. |
| **Daylight Saving Time Offset in Minutes** | Use this pull-down menu to specify the amount of time that will constitute your local DST offset – 30, 60, 90, or 120 minutes. |
| **Time Zone Offset from GMT in +/- HH:MM** | Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.) |
| *DST Repeating Settings* | Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October. |
| **From: Which Day** | Should be From: Which Week. Enter the week of the month that DST will start. |

| | |
|---|---|
| **From: Day of Week** | Enter the day of the week that DST will start on. |
| **From: Month** | Enter the month DST will start on. |
| **From: time in HH:MM** | Enter the time of day that DST will start on. |
| **To: Which Day** | Should be be To: Which Week. Enter the week of the month the DST will end. |
| **To: Day of Week** | Enter the day of the week that DST will end. |
| **To: Month** | Enter the month that DST will end. |
| **To: time in HH:MM** | Enter the time DST will end. |
| *DST Annual Settings* | Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14. |
| **From: Month** | Enter the month DST will start on, each year. |
| **From: Day** | Enter the day of the week DST will start on, each year. |
| **From: Time in HH:MM** | Enter the time of day DST will start on, each year. |
| **To: Month** | Enter the month DST will end on, each year. |
| **To: Day** | Enter the day of the week DST will end on, each year. |
| **To: Time in HH:MM** | Enter the time of day that DST will end on, each year. |

Click *Apply* to implement changes made to the **Time Zone and DST** window.

# Port Security

A given port's (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. The port can be locked by using the **Admin State** <*Disabled*> pull-down menu to *Enabled*, and clicking *Apply*.
This is a security feature that prevents unauthorized computers (with source MAC addresses unknown to the Switch prior to locking the port or ports) from connecting to the Switch's locked ports and gaining access to the network.

**Port Security Settings**

| From | To | Admin State | Max. Learning Addr.(0-10) | Lock Address Mode | Apply |
|---|---|---|---|---|---|
| Port 1 | Port 1 | Disabled | 1 | DeleteOnReset | Apply |

**Port Security Table**

| Port | Admin State | Max. Learning Addr. | Lock Address Mode |
|---|---|---|---|
| 1 | Disabled | 1 | DeleteOnReset |
| 2 | Disabled | 1 | DeleteOnReset |
| 3 | Disabled | 1 | DeleteOnReset |
| 4 | Disabled | 1 | DeleteOnReset |
| 5 | Disabled | 1 | DeleteOnReset |
| 6 | Disabled | 1 | DeleteOnReset |
| 7 | Disabled | 1 | DeleteOnReset |
| 8 | Disabled | 1 | DeleteOnReset |
| 9 | Disabled | 1 | DeleteOnReset |
| 10 | Disabled | 1 | DeleteOnReset |
| 11 | Disabled | 1 | DeleteOnReset |
| 12 | Disabled | 1 | DeleteOnReset |
| 13 | Disabled | 1 | DeleteOnReset |
| 14 | Disabled | 1 | DeleteOnReset |
| 15 | Disabled | 1 | DeleteOnReset |
| 16 | Disabled | 1 | DeleteOnReset |
| 17 | Disabled | 1 | DeleteOnReset |
| 18 | Disabled | 1 | DeleteOnReset |
| 19 | Disabled | 1 | DeleteOnReset |
| 20 | Disabled | 1 | DeleteOnReset |
| 21 | Disabled | 1 | DeleteOnReset |
| 22 | Disabled | 1 | DeleteOnReset |
| 23 | Disabled | 1 | DeleteOnReset |
| 24 | Disabled | 1 | DeleteOnReset |
| 25 | Disabled | 1 | DeleteOnReset |
| 26 | Disabled | 1 | DeleteOnReset |
| 27 | Disabled | 1 | DeleteOnReset |
| 28 | Disabled | 1 | DeleteOnReset |
| 29 | Disabled | 1 | DeleteOnReset |
| 30 | Disabled | 1 | DeleteOnReset |
| 31 | Disabled | 1 | DeleteOnReset |
| 32 | Disabled | 1 | DeleteOnReset |
| 33 | Disabled | 1 | DeleteOnReset |
| 34 | Disabled | 1 | DeleteOnReset |
| 35 | Disabled | 1 | DeleteOnReset |
| 36 | Disabled | 1 | DeleteOnReset |
| 37 | Disabled | 1 | DeleteOnReset |
| 38 | Disabled | 1 | DeleteOnReset |
| 39 | Disabled | 1 | DeleteOnReset |
| 40 | Disabled | 1 | DeleteOnReset |
| 41 | Disabled | 1 | DeleteOnReset |
| 42 | Disabled | 1 | DeleteOnReset |
| 43 | Disabled | 1 | DeleteOnReset |
| 44 | Disabled | 1 | DeleteOnReset |
| 45 | Disabled | 1 | DeleteOnReset |
| 46 | Disabled | 1 | DeleteOnReset |
| 47 | Disabled | 1 | DeleteOnReset |
| 48 | Disabled | 1 | DeleteOnReset |
| 49 | Disabled | 1 | DeleteOnReset |
| 50 | Disabled | 1 | DeleteOnReset |

**Figure 6- 27. Port Security Settings window**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **From/To** | A consecutive group of ports may be configured starting with the selected port. |
| **Admin State** | This pull-down menu allows you to **Enable** or **Disable** Port Security (locked MAC address table for the selected ports). |
| **Max.Addr(0-10)** | The number of MAC addresses that will be in the MAC address forwarding table for the selected switch and group of ports. |
| **Mode** | This pull-down menu allows you to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are **DeleteOnReset**, **DeleteOnTimeout**, and Permanent. |

Click *Apply* to implement the changes on the Switch.

# QoS

## Understanding QoS

The DES-3550 supports 802.1p priority queuing. The Switch has four priority queues. These priority queues are labeled as 3, the high queue, to 0, the lowest queue. The eight priority tags, specified in IEEE 802.1p are mapped to the Switch's priority tags as follows:

- Priority 0 is assigned to the Switch's Q1 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q0 queue.
- Priority 3 is assigned to the Switch's Q1 queue.
- Priority 4 is assigned to the Switch's Q2 queue.
- Priority 5 is assigned to the Switch's Q2 queue.
- Priority 6 is assigned to the Switch's Q3 queue.
- Priority 7 is assigned to the Switch's Q3 queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Multiple strict priority queues empty based on their priority tags. Only when these queues are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of 8 CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

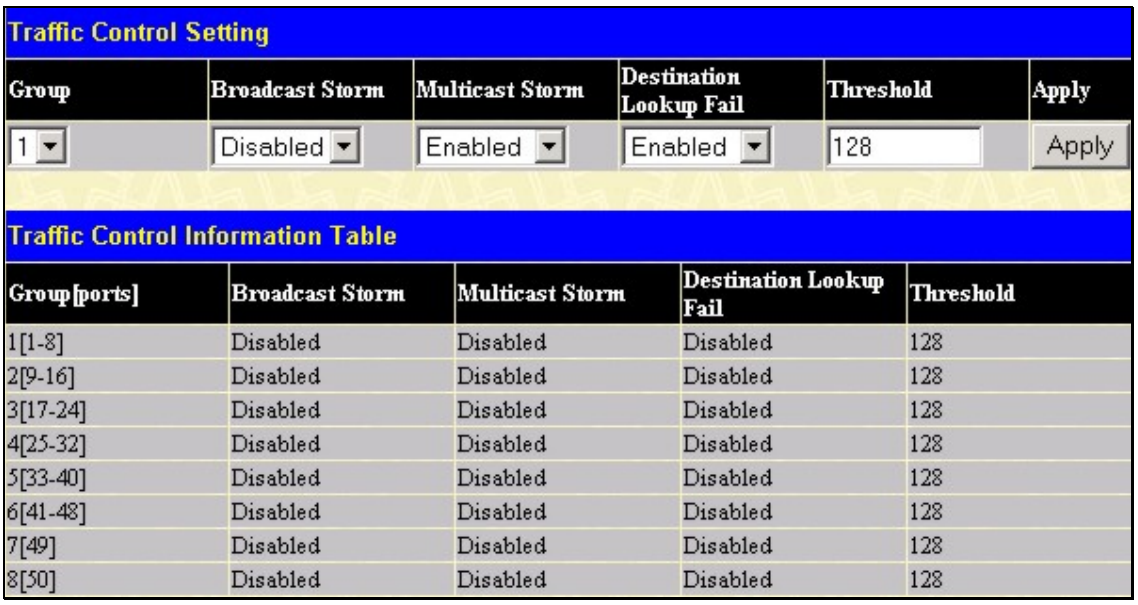
For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the DES-3550 has 4 priority queues (and four Classes of Service) for each port on the Switch.

## Traffic Control

Use the **Traffic Control** menu to enable or disable storm control and adjust the threshold for multicast and broadcast storms, as well as DLF (Destination Look Up Failure). Traffic control settings are applied to individual Switch modules. To view the following window, Open the QoS folder and click the **Traffic control** link:



Traffic Control Setting

| Group | Broadcast Storm | Multicast Storm | Destination Lookup Fail | Threshold | Apply |
|---|---|---|---|---|---|
| 1 | Disabled | Enabled | Enabled | 128 | Apply |

Traffic Control Information Table

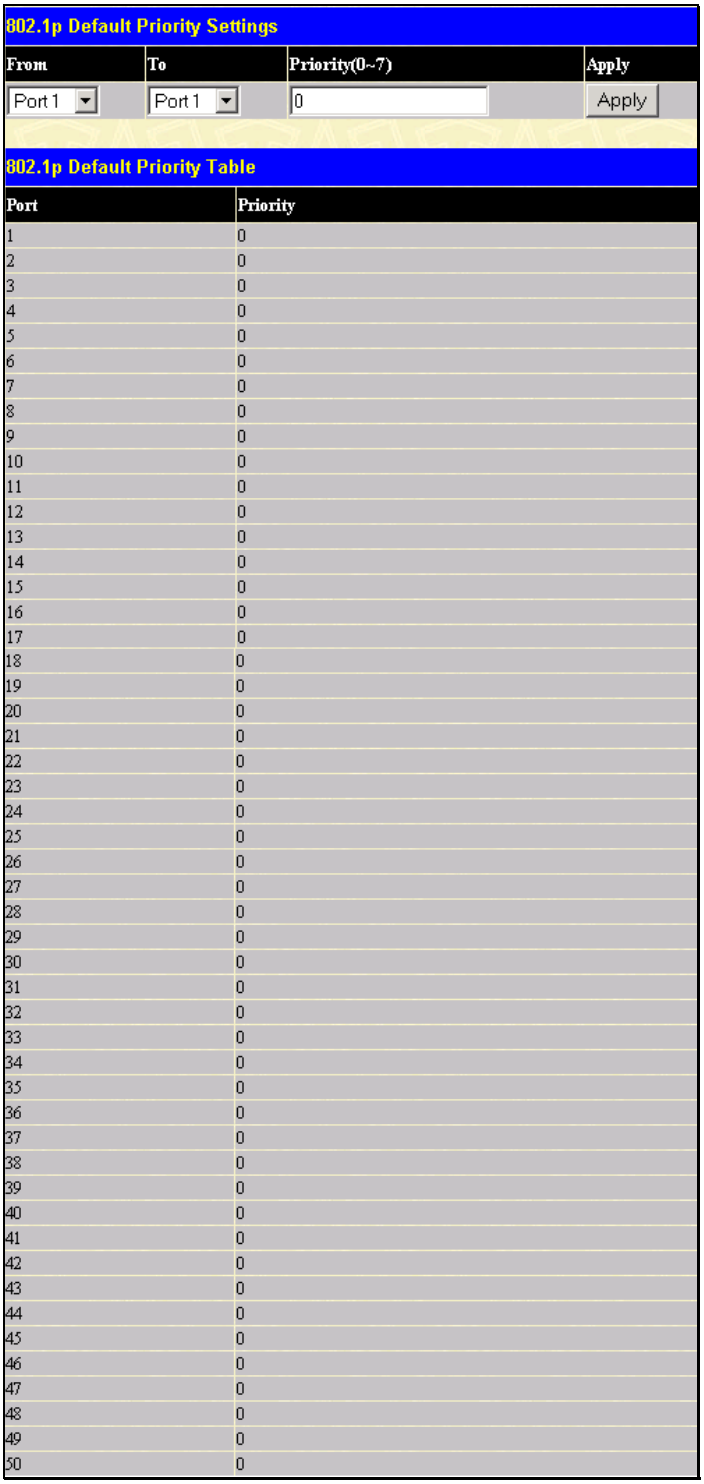
| Group[ports] | Broadcast Storm | Multicast Storm | Destination Lookup Fail | Threshold |
|---|---|---|---|---|
| 1[1-8] | Disabled | Disabled | Disabled | 128 |
| 2[9-16] | Disabled | Disabled | Disabled | 128 |
| 3[17-24] | Disabled | Disabled | Disabled | 128 |
| 4[25-32] | Disabled | Disabled | Disabled | 128 |
| 5[33-40] | Disabled | Disabled | Disabled | 128 |
| 6[41-48] | Disabled | Disabled | Disabled | 128 |
| 7[49] | Disabled | Disabled | Disabled | 128 |
| 8[50] | Disabled | Disabled | Disabled | 128 |

**Figure 6- 28. Traffic Control Settings and Traffic Control Table window**

Traffic or storm control is used to stop broadcast, multicast, or ARP request storms that may result when a loop is created. The **Destination Look Up Failure** control is a method of shutting down a loop when a storm is formed because a MAC address cannot be located in the Switch's forwarding database and it must send a packet to all ports or all ports on a VLAN.
To configure Traffic Control, first select a group of ports by using the **Group** pull down menu. As seen in the figure above, this section is set by 8 specified groups of ports on the Switch. **Group 1** refers to ports 1 through 8; **Group 2** refers to ports 9 through 16; **Group 3** refers to ports 17 through 24; **Group 4** refers to ports 25 through 32; **Group 5** refers to ports 33 through 40; **Group 6** refers to ports 41 through 48; **Group 7** refers to mini GBIC port 49; **Group 8** refers to mini GBIC port 50. **Broadcast Storm**, **Multicast Storm**, and **Destination Unknown** may be *Enabled* or *Disabled* for either group. The **Threshold** value is the upper threshold at which the specified traffic control is switched on. This is the number of Broadcast, Multicast, or DLF packets, in Kbps, received by the Switch that will trigger the storm traffic control measures. The Threshold value can be set from 0 to 255 packets. The default setting is 128. The settings of each port may be viewed in the **Traffic Control Table** in the same window. Click *Apply* to implement changes made.

## 802.1p Default Priority

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. In the **Configuration** folder open the **QoS** folder and click **802.1p Default Priority**, to view the screen shown below.



802.1p Default Priority Settings

| From | To | Priority(0~7) | Apply |
|---|---|---|---|
| Port 1 | Port 1 | 0 | Apply |

802.1p Default Priority Table

| Port | Priority |
|---|---|
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |
| 6 | 0 |
| 7 | 0 |
| 8 | 0 |
| 9 | 0 |
| 10 | 0 |
| 11 | 0 |
| 12 | 0 |
| 13 | 0 |
| 14 | 0 |
| 15 | 0 |
| 16 | 0 |
| 17 | 0 |
| 18 | 0 |
| 19 | 0 |
| 20 | 0 |
| 21 | 0 |
| 22 | 0 |
| 23 | 0 |
| 24 | 0 |
| 25 | 0 |
| 26 | 0 |
| 27 | 0 |
| 28 | 0 |
| 29 | 0 |
| 30 | 0 |
| 31 | 0 |
| 32 | 0 |
| 33 | 0 |
| 34 | 0 |
| 35 | 0 |
| 36 | 0 |
| 37 | 0 |
| 38 | 0 |
| 39 | 0 |
| 40 | 0 |
| 41 | 0 |
| 42 | 0 |
| 43 | 0 |
| 44 | 0 |
| 45 | 0 |
| 46 | 0 |
| 47 | 0 |
| 48 | 0 |
| 49 | 0 |
| 50 | 0 |

**Figure 6- 29. 802.1p Default Priority window**

This page allows you to assign a default 802.1p priority to any given port on the Switch. The priority queues are numbered from 0, the lowest priority, to 7, the highest priority. Click *Apply* to implement your settings.

## 802.1p User Priority

The DES-3550 allows the assignment of a user priority to each of the 802.1p priorities. In the **Configuration** folder open the **QoS** folder and click **802.1p User Priority**, to view the screen shown below.

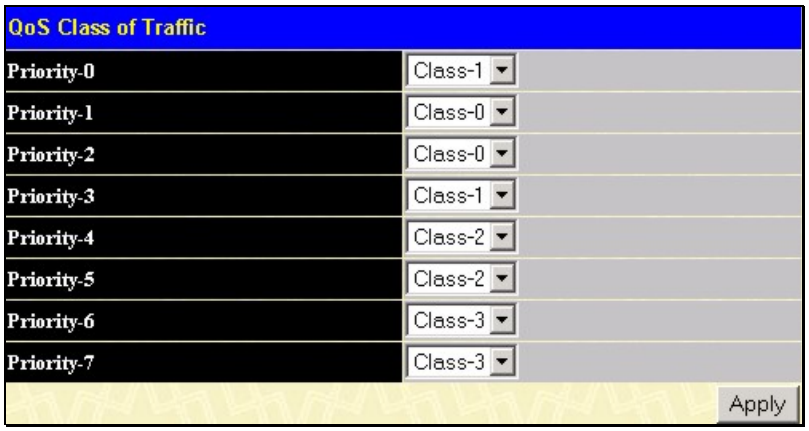



**Figure 6- 30. QoS Class of Traffic window**

Once you have assigned a priority to the port groups on the Switch, you can then assign this Class to each of the 4 levels of 802.1p priorities. Click *Apply* to set your changes.

## Scheduling

QoS can be customized by changing the output scheduling used for the hardware queues in the Switch. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If you choose to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable. In the **Configuration** folder open the **QoS** folder and click **QoS Output Scheduling**, to view the screen shown below.

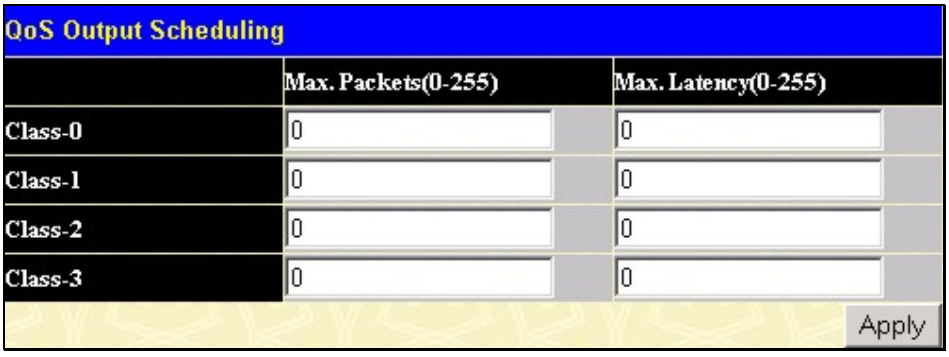



**Figure 6- 31. QoS Output Scheduling Configuration window**

You may assign the following values to the QoS classes to set the scheduling.

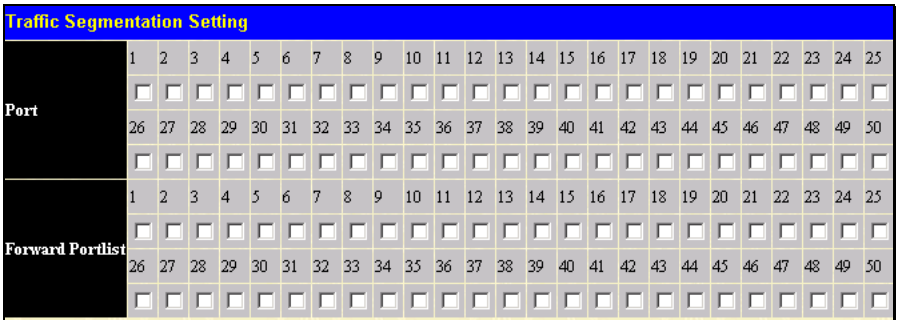
| Parameter | Description |
|---|---|
| **Max. Packets(0-255)** | Specifies the maximum number of packets the above specified hardware |

| | |
|---|---|
| | priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 255 can be specified. |
| **Max. Latency(0-255)** | Specifies the maximum amount of time the above specified hardware priority queue will be allowed to transmit packets before allowing the next lowest hardware priority queue to begin transmitting its packets. A value between 0 and 255 can be specified, with this value multiplied by 16 ms to arrive at the total allowed time for the queue to transmit packets. For example, a value of 3 specifies 3 X 16 = 48 ms. The queue will continue transmitting the last packet until it is finished when the max latency timer expires. |

**Note**: The settings you assign to the queues, numbers 0-7, represent the IEEE 802.1p priority tag number. Do not confuse these settings with port numbers.

## Traffic Segmentation

Traffic segmentation is used to limit traffic flow from a single port to a group of ports on either a single switch (in standalone mode) or a group of ports on another switch in a switch stack (Single IP). This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the Master switch CPU.
In the **Configuration** folder open the **QoS** folder and click **Traffic Segmentation**, to view the screen shown below.




**Traffic Segmentation Table**

| Port | Forward Portlist |
|---|---|
| 1 | 1-50 |
| 2 | 1-50 |
| 3 | 1-50 |
| 4 | 1-50 |
| 5 | 1-50 |
| 6 | 1-50 |
| 7 | 1-50 |
| 8 | 1-50 |
| 9 | 1-50 |
| 10 | 1-50 |
| 11 | 1-50 |
| 12 | 1-50 |
| 13 | 1-50 |
| 14 | 1-50 |
| 15 | 1-50 |
| 16 | 1-50 |
| 17 | 1-50 |
| 18 | 1-50 |
| 19 | 1-50 |
| 20 | 1-50 |
| 21 | 1-50 |
| 22 | 1-50 |
| 23 | 1-50 |
| 24 | 1-50 |
| 25 | 1-50 |
| 26 | 1-50 |
| 27 | 1-50 |
| 28 | 1-50 |
| 29 | 1-50 |
| 30 | 1-50 |
| 31 | 1-50 |
| 32 | 1-50 |
| 33 | 1-50 |
| 34 | 1-50 |
| 35 | 1-50 |
| 36 | 1-50 |
| 37 | 1-50 |
| 38 | 1-50 |
| 39 | 1-50 |
| 40 | 1-50 |
| 41 | 1-50 |
| 42 | 1-50 |
| 43 | 1-50 |
| 44 | 1-50 |
| 45 | 1-50 |
| 46 | 1-50 |
| 47 | 1-50 |
| 48 | 1-50 |
| 49 | 1-50 |
| 50 | 1-50 |

**Figure 6- 32. Traffic Segmentation Setting and Traffic Segmentation Table window**

This page allows you to determine which port on a given switch will be allowed to forward packets to other ports on that switch.
The user may set the following parameters:

| Parameter | Description |
|---|---|
| **Port** | Check the corresponding boxes for the port(s) you wish to transmit packets. |
| **Forward Portlist** | Check the boxes to select which of the ports on the selected switch will be able to forward packets. These are the ports that will be allowed to receive packets from the port specified above. |

Clicking the *Apply* button will enter the combination of transmitting port and allowed receiving ports into the Switch's **Traffic Segmentation Table**.

# MAC Notification

MAC Notification is used to monitor MAC addresses learned and entered into the forwarding database.

## Global Settings

To globally set MAC notification on the Switch, open the following screen by opening the **MAC Notification** folder and clicking the **Global Settings** link:

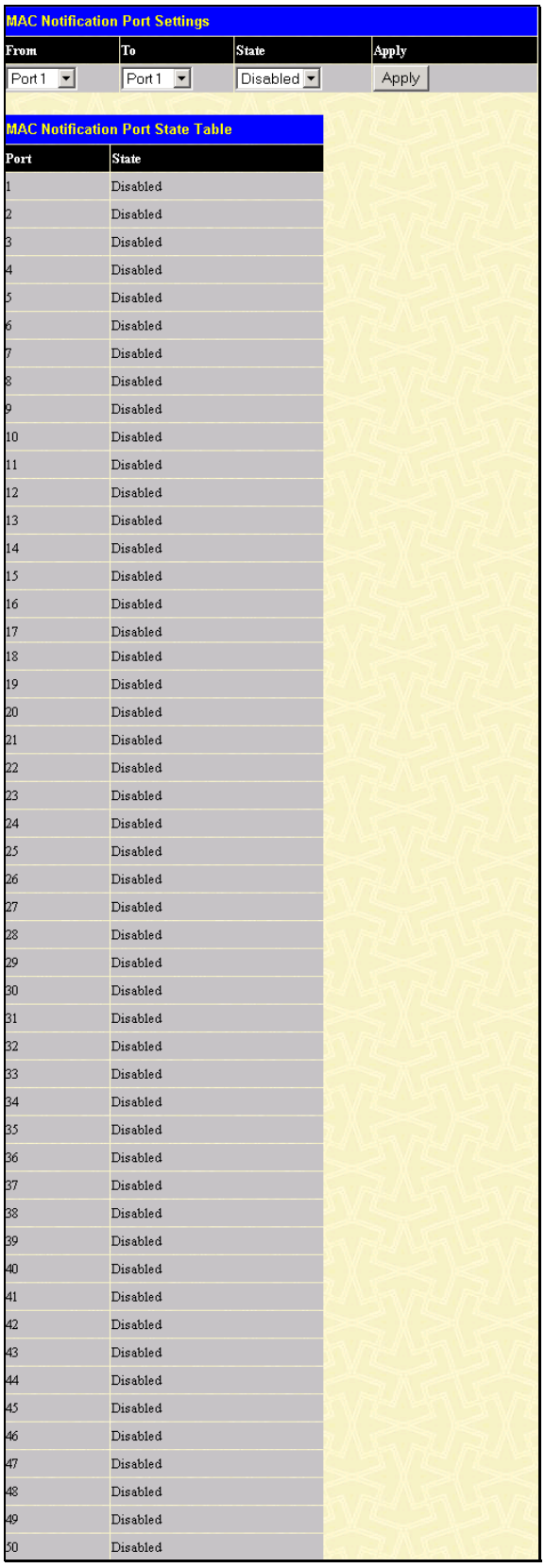
**Figure 6- 33. MAC Notification Global Setting window.**

The following parameters may be modified:

| Parameter | Description |
|---|---|
| **State** | Enable or disable MAC notification globally on the Switch |
| **Interval (sec)** | The time in seconds between notifications. |
| **History size** | The maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified. |

## Port Settings

To change MAC Notification settings for a port or group of ports on the Switch, click **Port Settings** in the **MAC Notification** folder, which will display the following screen:



MAC Notification Port Settings

| From | To | State | Apply |
|---|---|---|---|
| Port 1 | Port 1 | Disabled | Apply |

MAC Notification Port State Table

| Port | State |
|---|---|
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |
| 5 | Disabled |
| 6 | Disabled |
| 7 | Disabled |
| 8 | Disabled |
| 9 | Disabled |
| 10 | Disabled |
| 11 | Disabled |
| 12 | Disabled |
| 13 | Disabled |
| 14 | Disabled |
| 15 | Disabled |
| 16 | Disabled |
| 17 | Disabled |
| 18 | Disabled |
| 19 | Disabled |
| 20 | Disabled |
| 21 | Disabled |
| 22 | Disabled |
| 23 | Disabled |
| 24 | Disabled |
| 25 | Disabled |
| 26 | Disabled |
| 27 | Disabled |
| 28 | Disabled |
| 29 | Disabled |
| 30 | Disabled |
| 31 | Disabled |
| 32 | Disabled |
| 33 | Disabled |
| 34 | Disabled |
| 35 | Disabled |
| 36 | Disabled |
| 37 | Disabled |
| 38 | Disabled |
| 39 | Disabled |
| 40 | Disabled |
| 41 | Disabled |
| 42 | Disabled |
| 43 | Disabled |
| 44 | Disabled |
| 45 | Disabled |
| 46 | Disabled |
| 47 | Disabled |
| 48 | Disabled |
| 49 | Disabled |
| 50 | Disabled |

**Figure 6- 34. MAC Notification Port Settings and Port State Table**

The following parameters may be set:

| Parameter | Description |
|---|---|
| **From…To** | Select a port or group of ports to enable for MAC notification using the pull down menus. |
| **State** | Enable MAC Notification for the ports selected using the pull down menu. |

Click *Apply* to implement changes made.

# LACP

## Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline.

The DES-3550 supports up to 6 port trunk groups with 2 to 8 ports in each group. A potential bit rate of 8000 Mbps can be achieved.

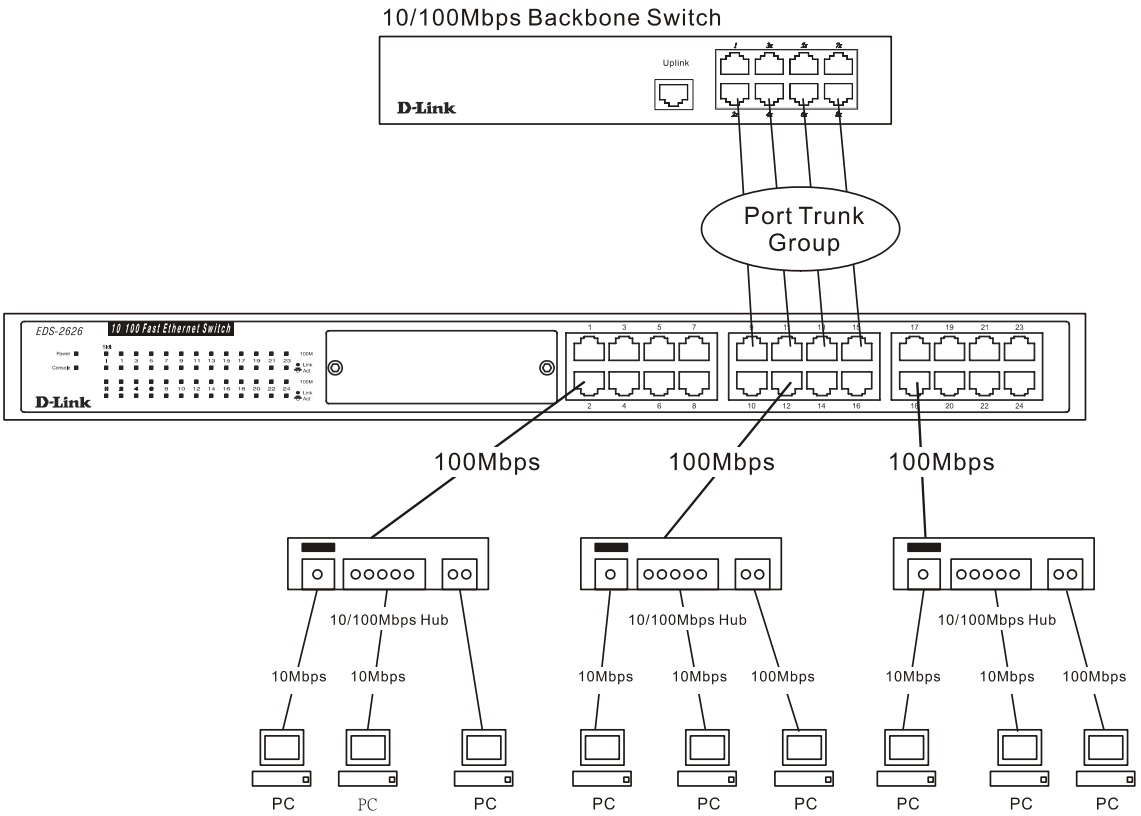



**Figure 6- 35. Example of Port Trunk Group**

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

**Note**: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other uplinked ports of the link aggregation group.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.
Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.
The Switch allows the creation of up to 6 link aggregation groups, each group consisting of 2 to 8 links (ports). The aggregated links must be contiguous (they must have sequential port numbers) except the two (optional) Gigabit ports, which can only belong to a single link aggregation group. All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control, traffic segmentation, and 802.1p default priority configurations must be identical. Port locking, port mirroring, and 802.1X must not be enabled on the trunk group. Further, the aggregated links must all be of the same speed and should be configured as full-duplex.
The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration, that can be applied to the Master Port are applied to the entire link aggregation group.
Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.
The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group, in the same way STP will block a single port that has a redundant link.
To configure port trunking, click on the **Link Aggregation** hyperlink in the **Configuration** folder to bring up the **Current Link Aggregation Group Entries** table:

**Figure 6- 36. Port Link Aggregation Group Entries window**

To configure port trunk groups, click the *Add* button to add a new trunk group and use the menu **Link Aggregation Group Configuration** menu (see example below) to set up trunk groups. To modify a port trunk group, click the Modify button corresponding to the entry you wish to alter. To delete a port trunk group, click the corresponding ✕ under the **Delete** heading in the **Current Link Aggregation Group Entries** table.

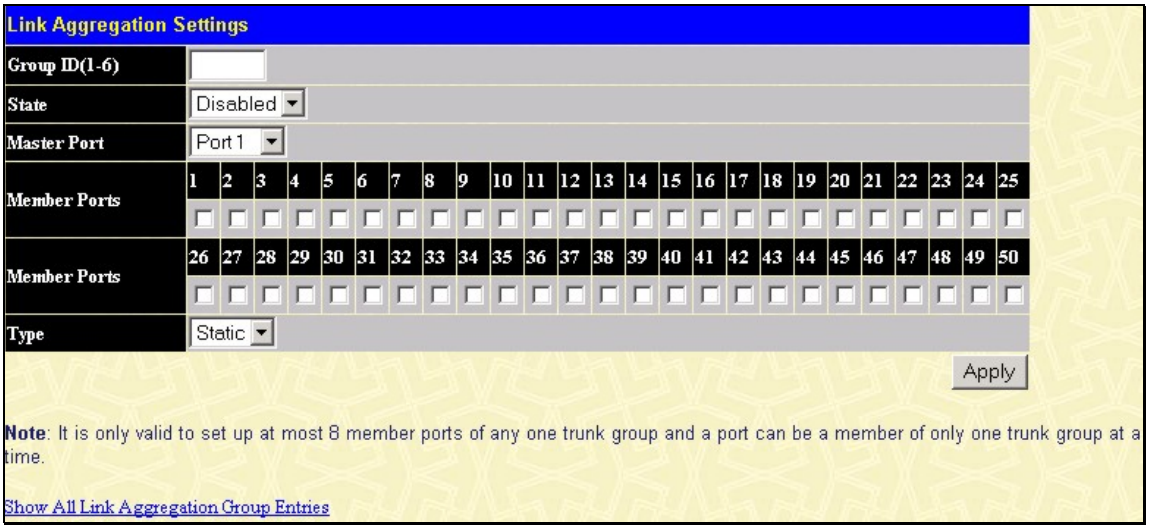

Link Aggregation Settings
Group ID(1-6)
State
Disabled
Master Port
Port 1
Member Ports
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
Member Ports
26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
Type
Static
Apply
Note: It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.
Show All Link Aggregation Group Entries

**Figure 6- 37. Link Aggregation Settings window – Add**

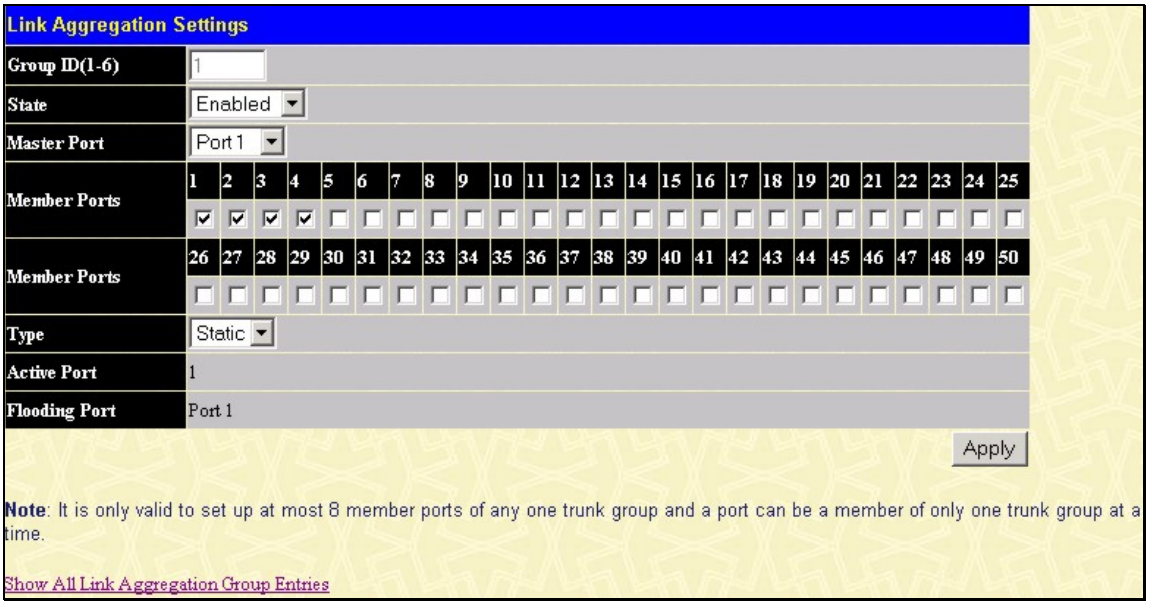

Link Aggregation Settings
Group ID(1-6)
1
State
Enabled
Master Port
Port 1
Member Ports
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
Member Ports
26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
Type
Static
Active Port
1
Flooding Port
Port 1
Apply
Note: It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.
Show All Link Aggregation Group Entries

**Figure 6- 38. Link Aggregation Group Configuration window – Modify**

The user-changeable parameters are as follows:

| Parameter | Description |
|---|---|
| **Group ID** | Select an ID number for the group, between 1 and 6. |
| **State** | Trunk groups can be toggled between *Enabled* and *Disabled*. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control. |
| **Master Port** | Choose the Master port for the trunk group. |
| **Member Ports** | Choose the members of a trunked group. Up to 8 ports per group can be assigned to a group. |

| | |
|---|---|
| **Flooding Port** | A trunking group must designate one port to allow transmission of broadcasts and unknown unicasts. |
| **Active Port** | Shows the port that is currently forwarding packets. |
| **Type** | This pull-down menu allows you to select between *Static* and *LACP* (Link Aggregation Control Protocol). LACP allows for the automatic detection of links in a Port Trunking Group. |

After setting the previous parameters, click *Apply* to allow your changes to be implemented. Successfully created trunk groups will be shown in the **Current Link Aggregation Group Entries** as seen in Figure 6-36.

## LACP Port

The **LACP Port Setting** window is used in conjunction with the **Link Aggregation** window to create port trunking groups on the Switch. Using the following window, the user may set which ports will be active and passive in processing and sending LACP control frames.

**Lacp Port Settings**

| From | To | Mode | Apply |
|---|---|---|---|
| Port 1 | Port 1 | Passive | Apply |

**Lacp Port Table**

| Port | Activity |
|---|---|
| 1 | Passive |
| 2 | Passive |
| 3 | Passive |
| 4 | Passive |
| 5 | Passive |
| 6 | Passive |
| 7 | Passive |
| 8 | Passive |
| 9 | Passive |
| 10 | Passive |
| 11 | Passive |
| 12 | Passive |
| 13 | Passive |
| 14 | Passive |
| 15 | Passive |
| 16 | Passive |
| 17 | Passive |
| 18 | Passive |
| 19 | Passive |
| 20 | Passive |
| 21 | Passive |
| 22 | Passive |
| 23 | Passive |
| 24 | Passive |
| 25 | Passive |
| 26 | Passive |
| 27 | Passive |
| 28 | Passive |
| 29 | Passive |
| 30 | Passive |
| 31 | Passive |
| 32 | Passive |
| 33 | Passive |
| 34 | Passive |
| 35 | Passive |
| 36 | Passive |
| 37 | Passive |
| 38 | Passive |
| 39 | Passive |
| 40 | Passive |
| 41 | Passive |
| 42 | Passive |
| 43 | Passive |
| 44 | Passive |
| 45 | Passive |
| 46 | Passive |
| 47 | Passive |
| 48 | Passive |
| 49 | Passive |
| 50 | Passive |

**Figure 6- 39. Lacp Port Settings and LACP Port Table**

The user may set the following parameters:

| Parameter | Description |
|---|---|
| **From/To** | A consecutive group of ports may be configured starting with the selected port. |
| **Mode** | *Active* – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.<br>*Passive* – LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports (see above). |

After setting the previous parameters, click *Apply* to allow your changes to be implemented. The **LACP Port Table** shows which ports are active and/or passive.

# Access Profile Table

# Configuring the Access Profile Table

Access profiles allow you to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of VLAN, MAC address, or IP address.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

To display the currently configured Access Profiles on the Switch, open the **Configuration** folder and click on the **Access Profile Table** link. This will open the **Access Profile Table** page, as shown below.

**Figure 6- 40. Access Profile Table**

To add an entry to the **Access Profile Table**, click the *Add* button. This will open the **Access Profile Configuration** page, as shown below. There are three **Access Profile Configuration** pages: one for **Ethernet** (or MAC address-based) profile configuration, one for **IP** address-based profile configuration, and one for the **Packet Content Mask**. You can switch between the three **Access Profile Configuration** pages by using the **Type** drop-down menu. The page shown below is the **Ethernet Access Profile Configuration** page.

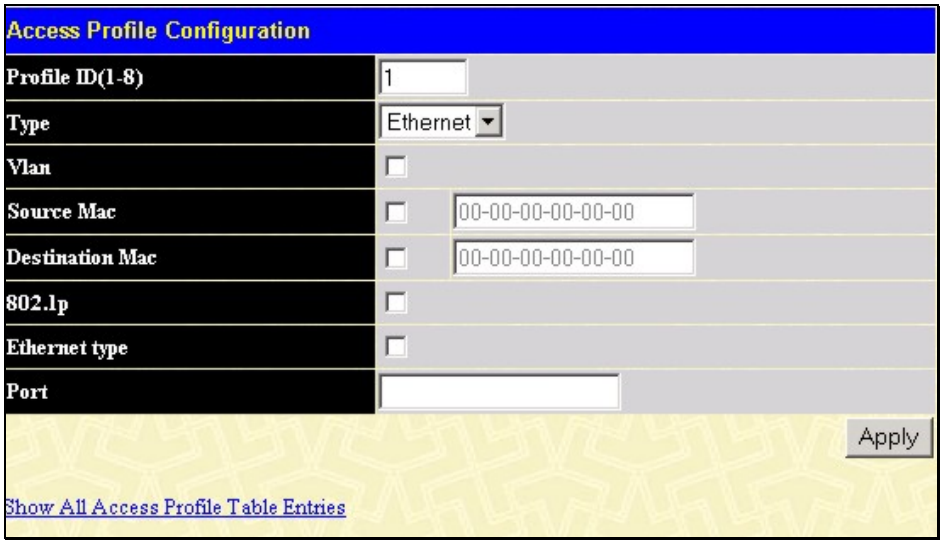



**Figure 6- 41. Access Profile Table (Ethernet)**

The following parameters can be set for Ethernet:

| Parameter | Description |
|---|---|
| **Profile ID (1-255)** | Type in a unique identifier number for this profile set. This value can be set from 1 – 255. |
| **Type** | Select profile based on Ethernet (MAC Address), IP address, or packet content mask. This will change the menu according to the requirements for the type of profile. Select **Ethernet** to instruct the Switch to examine the layer 2 part of each packet header. Select **IP** to instruct the Switch to examine the IP address in each frame's header. Select **Packet Content Mask** to specify a mask to hide the content of the packet header. |
| **Vlan** | Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the full or partial criterion for forwarding. |
| **Source Mac** | Source MAC Mask - Enter a MAC address mask for the source MAC address. |
| **Destination Mac** | Destination MAC Mask - Enter a MAC address mask for the destination MAC address. |
| **802.1p** | Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding. |
| **Ethernet type** | Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header. |
| **Port** | The user may set the **Access Profile Table** on a per-port basis by entering a port number in this field. |

The page shown below is the **IP Access Profile Configuration** page.

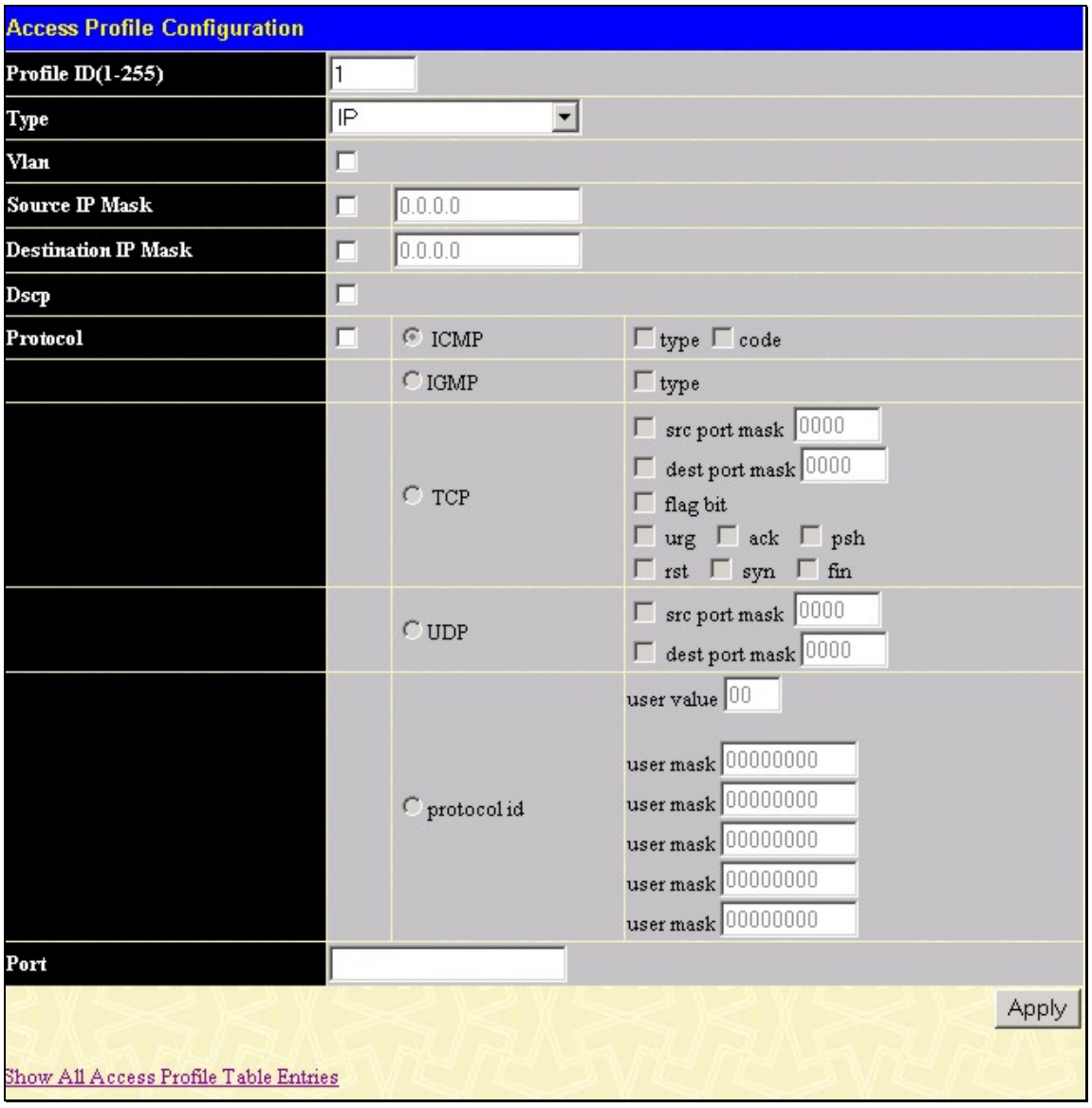



**Figure 6- 42. Access Profile Configuration (IP)**

The following parameters can be set for IP:

| Parameter | Description |
|---|---|
| **Profile ID(1-255)** | Type in a unique identifier number for this profile set. This value can be set from 1 – 255. |
| **Type** | Select profile based on Ethernet (MAC Address), IP address, or packet content mask. This will change the menu according to the requirements for the type of profile. Select **Ethernet** to instruct the Switch to examine the layer 2 part of each packet header. Select **IP** to instruct the Switch to examine the IP address in each frame's header. Select **Packet Content Mask** to specify a mask to hide the content of the packet header. |
| **Vlan** | Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding. |

| | |
|---|---|
| **Source IP Mask** | Source IP Mask - Enter an IP address mask for the source IP address. |
| **Destination IP Mask** | Destination IP Mask - Enter an IP address mask for the destination IP address. |
| **Dscp** | Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding. |
| **Protocol** | Selecting this option instructs the Switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines:<br>Select **ICMP** to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.<br>Select **Type** to further specify that the access profile will apply an ICMP type value, or specify **Code** to further specify that the access profile will apply an ICMP code value.<br>Select **IGMP** to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.<br>Select **Type** to further specify that the access profile will apply an IGMP type value.<br>Select **TCP** to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. The user may also identify which flag bits to deny. Flag bits are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between **urg** (urgent), **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize), and **fin** (finish).<br>**src port mask –** Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to deny.<br>**dest port mask –** Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to deny.<br>Select **UDP** to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask.<br>**src port mask** – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff).<br>**dest port mask** – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff).<br>**protocol id –** user value: Enter a value defining the protocol id in the packet header you wish to mask.<br>Specify up to 5, Layer 4 port masks for the destination port in hex form (hex 0x0-0xffffffff). |
| **Port** | The user may set the **Access Profile Table** on a per-port basis by entering an entry in this field. Entering all will denote all ports on the Switch. |

The page shown below is the **Packet Content Mask** configuration window.

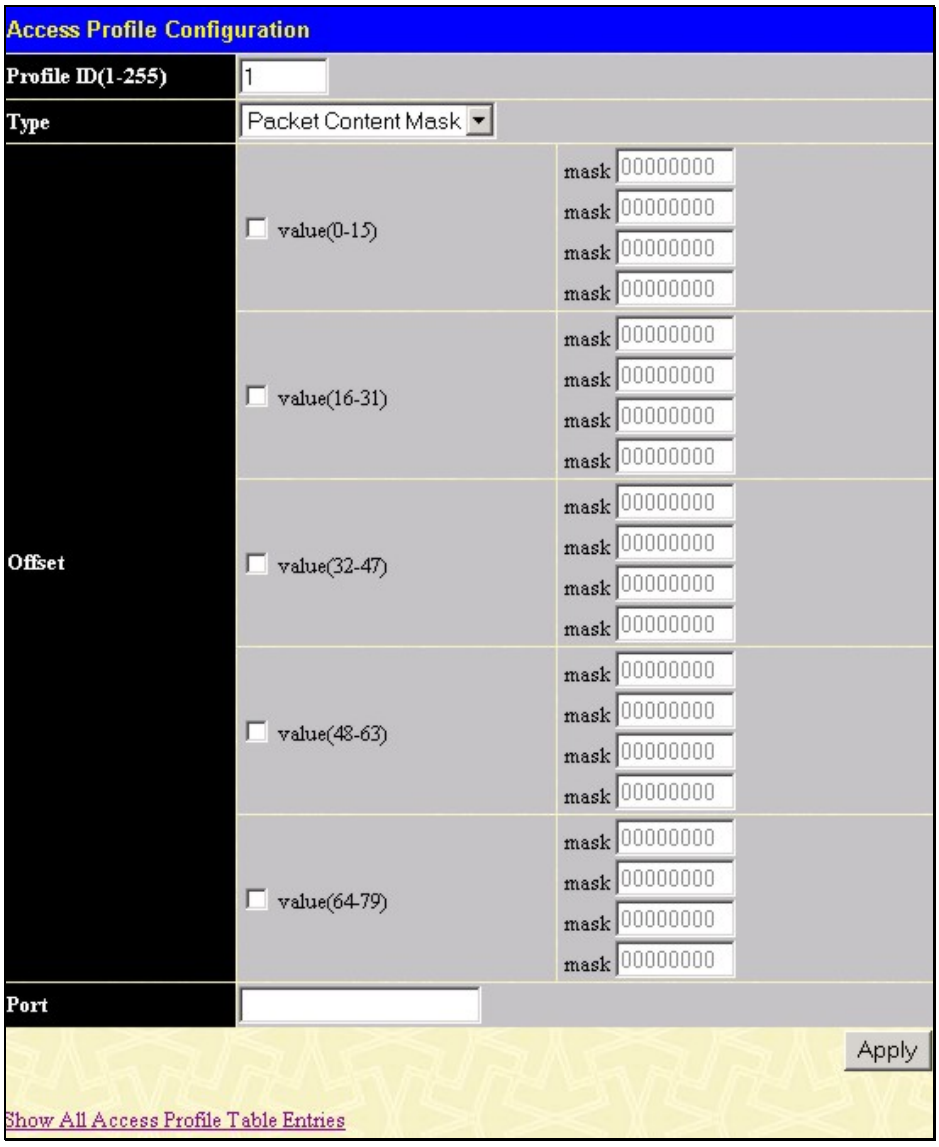



**Figure 6- 43. Access Profile Configuration window (Packet Content Mask)**

This screen will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the **Packet Content Masks**:

| Parameter | Description |
|---|---|
| **Profile ID(1-255)** | Type in a unique identifier number for this profile set. This value can be set from 1 – 255. |
| **Type** | Select profile based on Ethernet (MAC Address), IP address, or packet content mask. This will change the menu according to the requirements for the type of profile. Select **Ethernet** to instruct the Switch to examine the layer 2 part of each packet header. Select **IP** to instruct the Switch to examine the IP address in each frame's header. Select **Packet Content Mask** to specify a mask to hide the content of the packet header. |
| **Offset** | This field will instruct the Switch to mask the packet header beginning with |

| | |
|---|---|
| | the offset value specified:<br>value(0-15) - Enter a value in hex form to mask the packet from the beginning of the packet to the 16th byte.<br>value(16-31) - Enter a value in hex form to mask the packet from byte 16 to byte 31.<br>value(32-47) - Enter a value in hex form to mask the packet from byte 32 to byte 47.<br>value(48-63) - Enter a value in hex form to mask the packet from byte 48 to byte 63.<br>value(64-79) - Enter a value in hex form to mask the packet from byte 16 to byte 31. |
| **Port** | The user may set the **Access Profile Table** on a per-port basis by entering an entry in this field. Entering all will denote all ports on the Switch. |

Click *Apply* to implement changes made.

***To establish the rule for a previously created Access Profile:***

In the **Configuration** folder, click the **Access Profile Table** link opening the **Access Profile Table**. Under the heading **Access Rule**, clicking *Modify*, will open the following window.

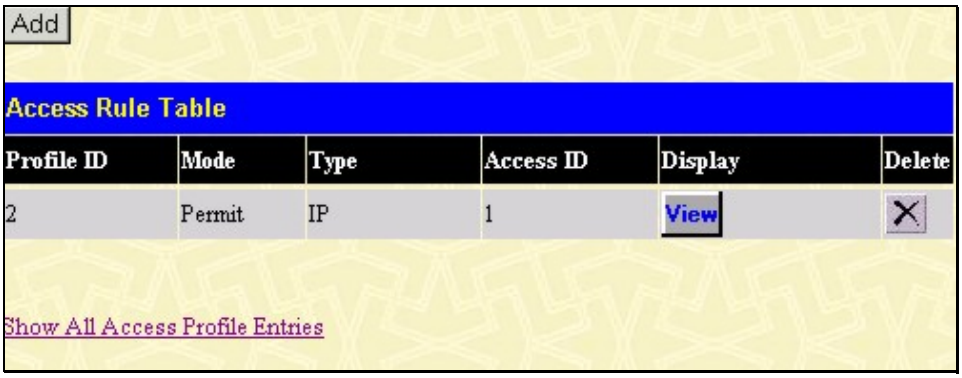



**Figure 6- 44. Access Rule Table window**

To create a new rule set for the access profile click the *Add* button. A new window is displayed. To remove a previously created rule, select it and click the button.

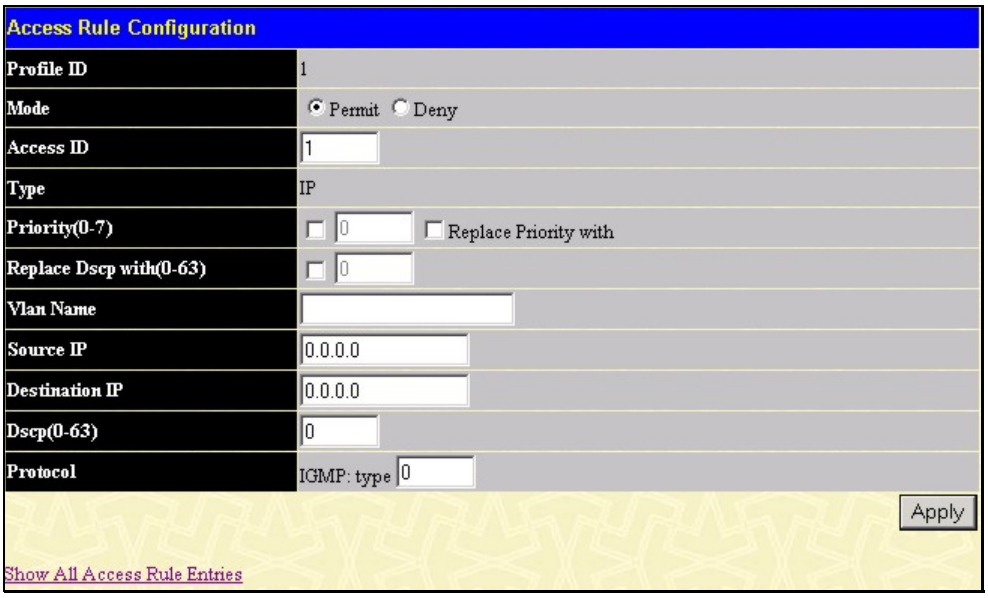



**Figure 6- 45. Access Rule Configuration window (IP)**

Configure the following **Access Rule Configuration** settings:

| Parameter | Description |
|---|---|
| **Profile ID** | This is the identifier number for this profile set. |
| **Mode** | Select **Permit** to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).<br>Select **Deny** to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered. |
| **Access ID** | Type in a unique identifier number for this access. This value can be set from 1 – 50. |
| **Type** | Selected profile based on Ethernet (MAC Address), IP address, or Packet Content Mask. Ethernet instructs the Switch to examine the layer 2 part of each packet header. IP instructs the Switch to examine the IP address in each frame's header. Packet Content Mask instructs the Switch to examine the packet header. |
| **Priority (0-7)** | Select this option to instruct the Switch to use the 802.1p priority value entered in the adjacent field for packets that meet the criteria. A number between 0, the lowest priority, and 7, the highest priority, can be entered. |
| **Replace Dscp (0-63)** | Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. |
| **Vlan Name** | Allows the entry of a name for a previously configured VLAN. |
| **Source IP** | Source IP Address - Enter an IP Address mask for the source IP address. |
| **Destination IP** | Destination IP Address- Enter an IP Address mask for the destination IP address. |

| | |
|---|---|
| **Dscp(0-63)** | This field allows the user to enter a Dscp value in the space provided, which will instruct the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding. The user may choose a value between 0 and 63. |
| **Protocol** | This field allows the user to modify the protocol used to configure the **Access Rule Table**; depending on which protocol the user has chosen in the Access Profile Table. In the example above, IGMP is the protocol chosen and therefore the user may modify the IGMP settings for this access profile. |

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** to view the following screen:

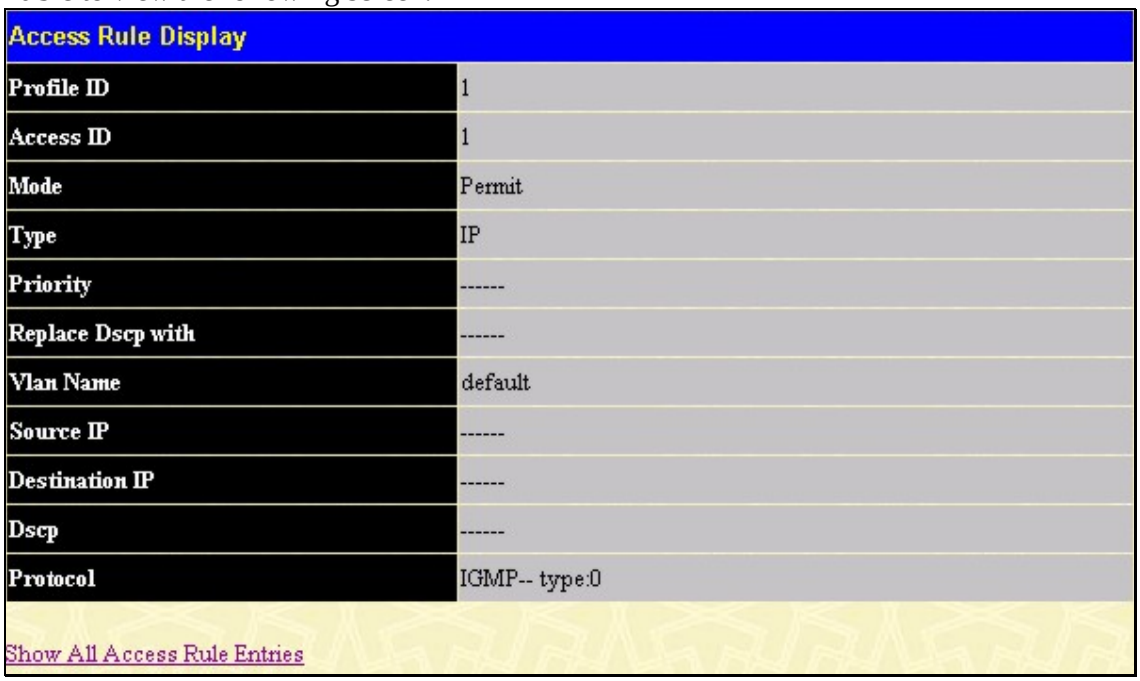



**Figure 6- 46. Access Rule Display window (IP)**

To configure the Access Rule for Ethernet, open the **Access Profile Table** (figure 6-40) and click *Modify* for an Ethernet entry. This will open the following screen:

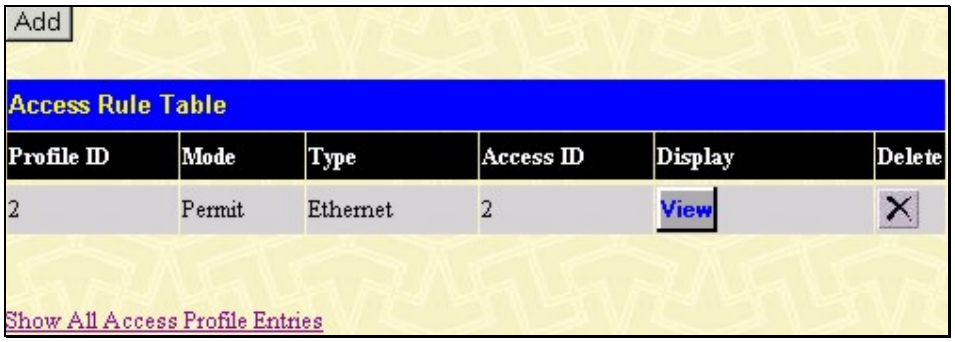



**Figure 6- 47. Access Rule Table**

To remove a previously created rule, select it and click the button. To add a new Access Rule, click the *Add* button:

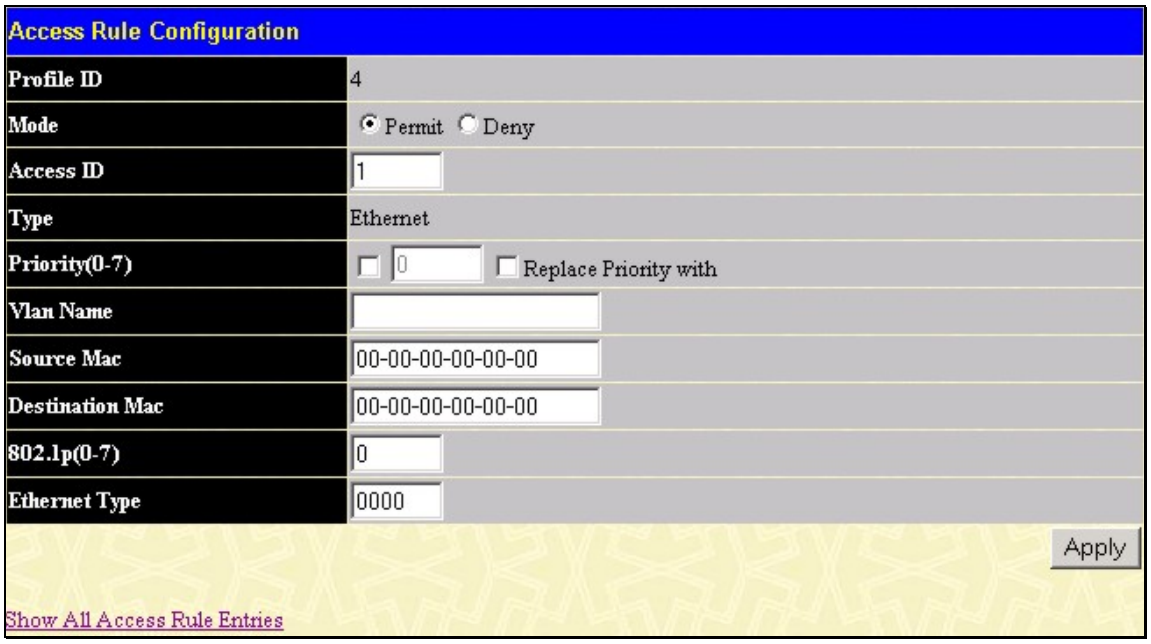



**Figure 6- 48. Access Rule Configuration window (Ethernet).**

To set the **Access Rule** for *Ethernet*, adjust the following parameters and click *Apply*.

| Parameters | Description |
|---|---|
| **Profile ID** | This is the identifier number for this profile set. |
| **Mode** | Select **Permit** to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).<br>Select **Deny** to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered. |
| **Access ID** | Type in a unique identifier number for this access. This value can be set from 1 – 50. |
| **Type** | Selected profile based on Ethernet (MAC Address), IP address, or Packet Content Mask. Ethernet instructs the Switch to examine the layer 2 part of each packet header. IP instructs the Switch to examine the IP address in each frame's header. Packet Content Mask instructs the Switch to examine the packet header. |
| **Priority(0-7)** | Select this option to instruct the Switch to use the 802.1p priority value entered in the adjacent field for packets that meet the criteria. A number between 0, the lowest priority, and 7, the highest priority, can be entered. |
| **Vlan Name** | Allows the entry of a name for a previously configured VLAN. |
| **Source Mac** | Source MAC Address - Enter a MAC Address for the source MAC address. |
| **Destination Mac** | Destination MAC Address - Enter a MAC Address mask for the destination MAC address. |

| | |
|---|---|
| **802.1p(0-7)** | Enter a value from 0-7 to specify that the access profile will apply only to packets with this 802.1p priority value. |
| **Ethernet Type** | Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form: hex 0x0-0xffff, which means the user may choose any combination of letters and numbers ranging from ***a-f*** and from ***0-9999***. |

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** to view the following screen:

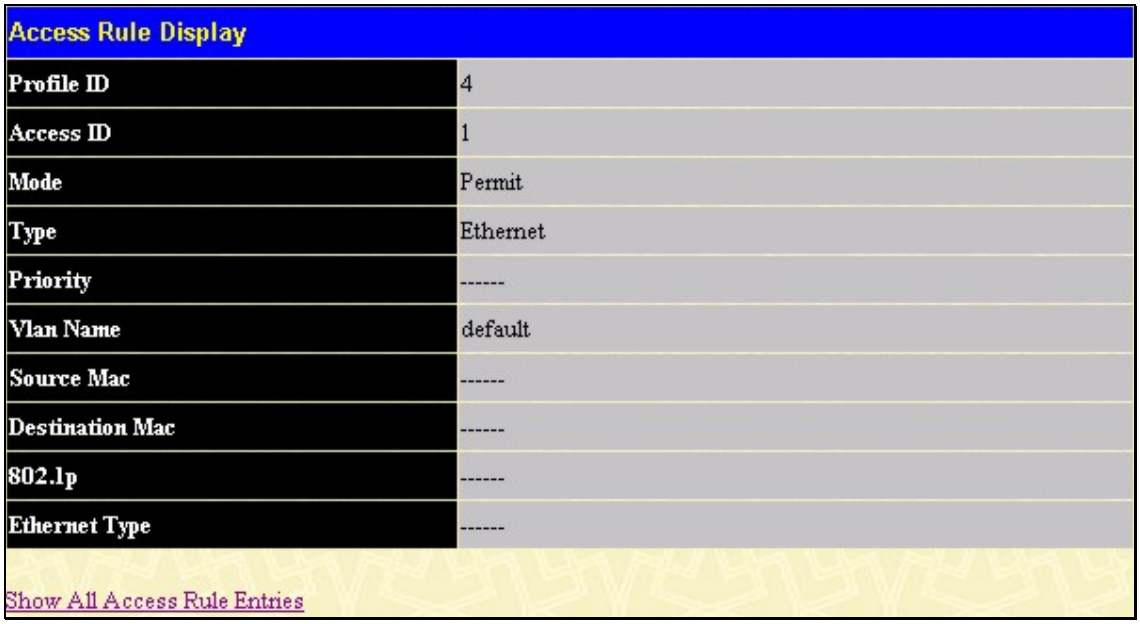



**Figure 6- 49. Access Rule Display window (Ethernet)**

To configure the Access Rule for Packet Content Mask, open the **Access Profile Table** (figure 6-35) and click *Modify* for an Ethernet entry. This will open the following screen:

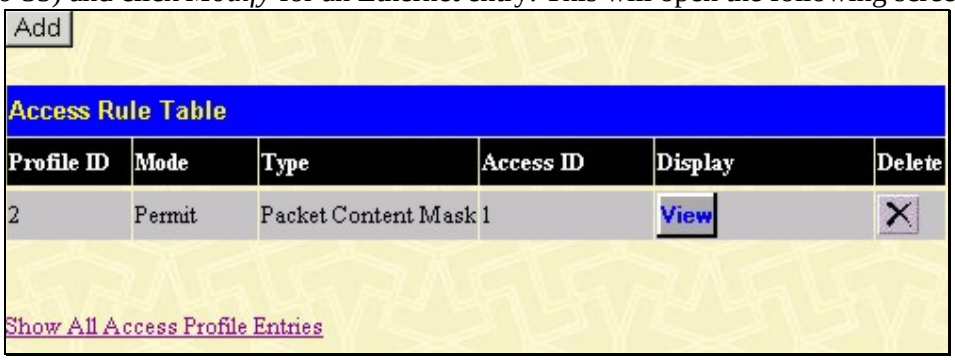



**Figure 6- 50. Access Rule Table (Packet Content Mask)**

To remove a previously created rule, select it and click the button. To add a new Access Rule, click the *Add* button:

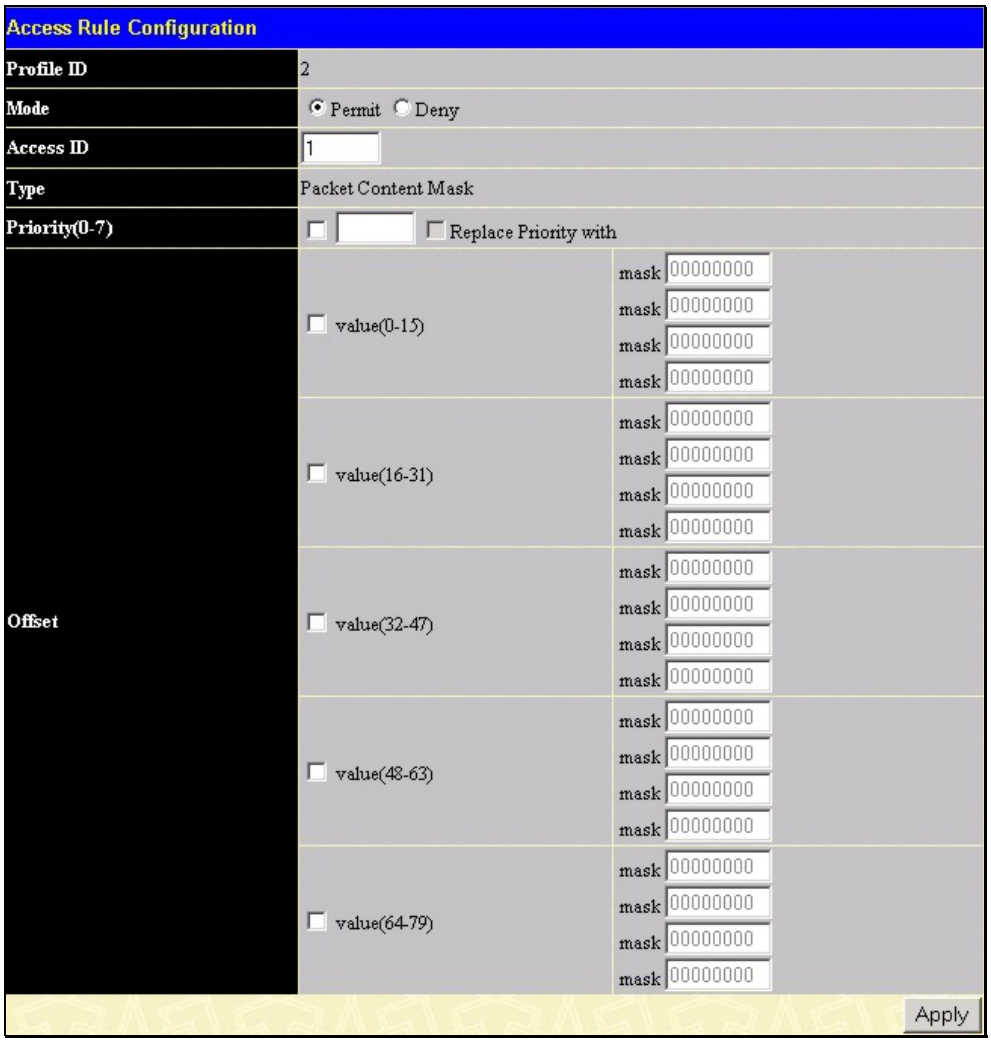



**Figure 6- 51. Access Rule Configuration (Packet Content Mask)**

To set the Access Rule for the **Packet Content Mask**, adjust the following parameters and click *Apply*.

| Parameter | Description |
|---|---|
| **Profile ID** | This is the identifier number for this profile set. |
| **Mode** | Select **Permit** to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).<br>Select **Deny** to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered. |
| **Access ID** | Type in a unique identifier number for this access. This value can be set from 1 – 50. |
| **Type** | Selected profile based on Ethernet (MAC Address), IP address, or Packet Content Mask. Ethernet instructs the Switch to examine the layer 2 part of each packet header. IP instructs the Switch to examine the IP address in each frame's header. Packet Content Mask instructs the Switch to examine the packet header. |

| | |
|---|---|
| **Priority** | Select this option to instruct the Switch to use the 802.1p priority value entered in the adjacent field for packets that meet the criteria. A number between 0, the lowest priority, and 7, the highest priority, can be entered. |
| **Offset** | This field will instruct the Switch to mask the packet header beginning with the offset value specified:<br>value(0-15) - Enter a value in hex form to mask the packet from the beginning of the packet to the 16th byte.<br>value(16-31) - Enter a value in hex form to mask the packet from byte 16 to byte 31.<br>value(32-47) - Enter a value in hex form to mask the packet from byte 32 to byte 47.<br>value(48-63) - Enter a value in hex form to mask the packet from byte 48 to byte 63.<br>value(64-79) - Enter a value in hex form to mask the packet from byte 16 to byte 31. |

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** to view the following screen:

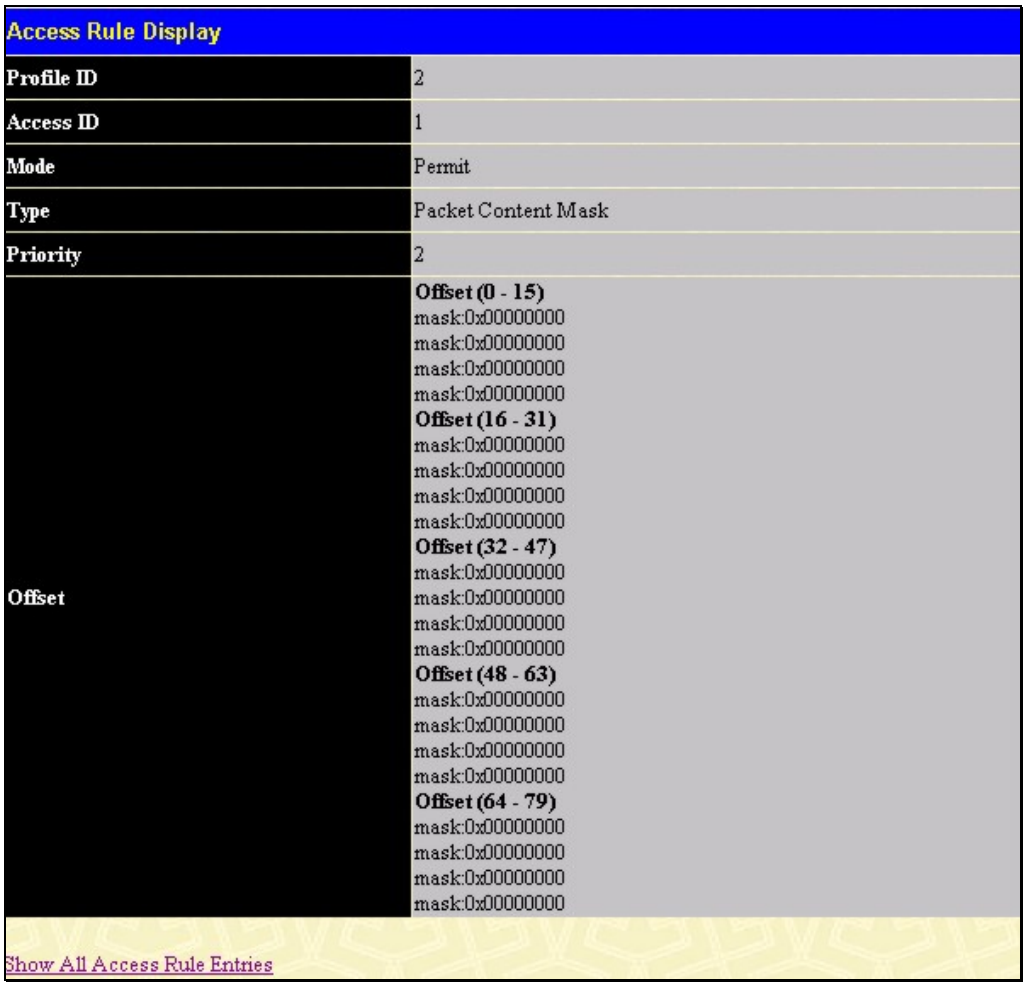



**Figure 6- 52. Access Rule Display window (Ethernet)**

## System Log Server

The Switch can send Syslog messages to up to four designated servers using the **System Log Server**. In the **Configuration** folder, click **System Log Server**, to view the screen shown below.

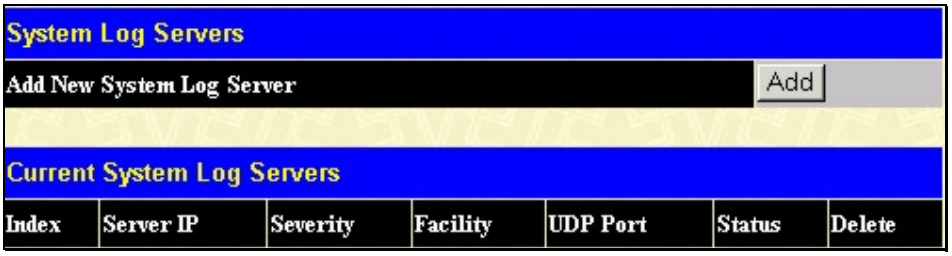



**Figure 6- 53. System Log Servers window**

The parameters configured for adding and editing **System Log Server** settings are the same. See the table below for a description.

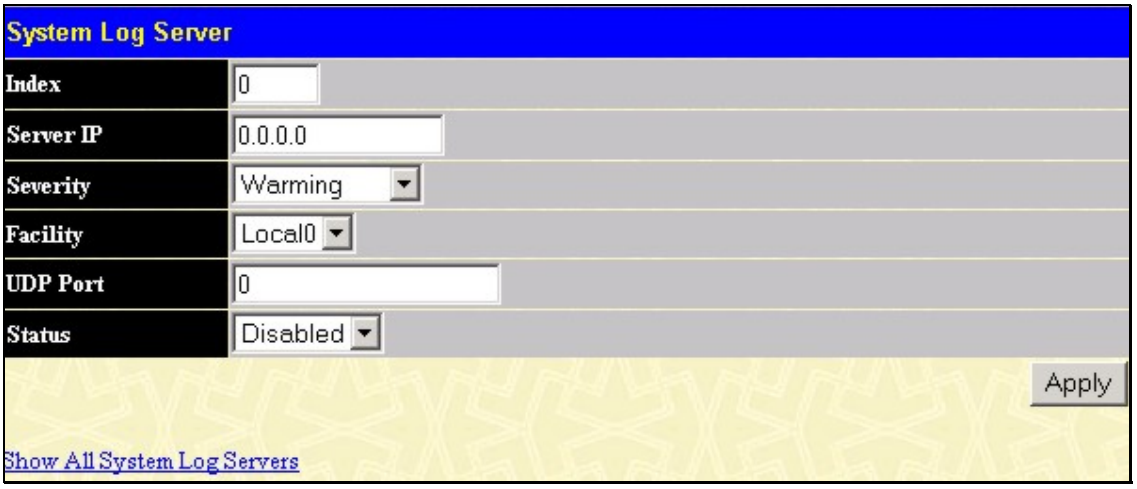



**Figure 6- 54. System Log Servers – Add**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **Index** | Syslog server settings index (1-4). |
| **Server IP** | The IP address of the Syslog server. |
| **Severity** | This drop-down menu allows you to select the level of messages that will be sent. The options are **Warning**, **Informational**, and **All**. |
| **Facility** | Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values that the Switch currently supports now. |

| | |
|---|---|
| | Numerical Code Facility<br>0 kernel messages<br>1 user-level messages<br>2 mail system<br>3 system daemons<br>4 security/authorization messages<br>5 messages generated internally by syslog line printer subsystem<br>7 network news subsystem<br>8 UUCP subsystem<br>9 clock daemon<br>10 security/authorization messages<br>11 FTP daemon<br>12 NTP subsystem<br>13 log audit<br>14 log alert<br>15 clock daemon<br>**16 local use 0 (local0)**<br>**17 local use 1 (local1)**<br>**18 local use 2 (local2)**<br>**19 local use 3 (local3)**<br>**20 local use 4 (local4)**<br>**21 local use 5 (local5)**<br>**22 local use 6 (local6)**<br>**23 local use 7 (local7)** |
| **UDP Port (514 or 6000-65535)** | Type the UDP port number used for sending Syslog messages. The default is 0. |
| **Status** | Choose *Enabled* or *Disabled* to activate or deactivate. |

To set the **System Log Server** configuration, click *Apply*. To delete an entry from the **System Log Server** window, click the corresponding ✕ under the **Delete** heading of the entry you wish to delete. To return to the Current System Log Servers window, click the Show All System Log Servers link.

# PAE Access Entity (802.1X)

## Understanding 802.1x Port-based Network Access Control

The Switch is an implementation of the server side of IEEE 802.1x Port-Based Network Access Control. Through this mechanism, users have to be authorized before being able to access the network. See the following figure:

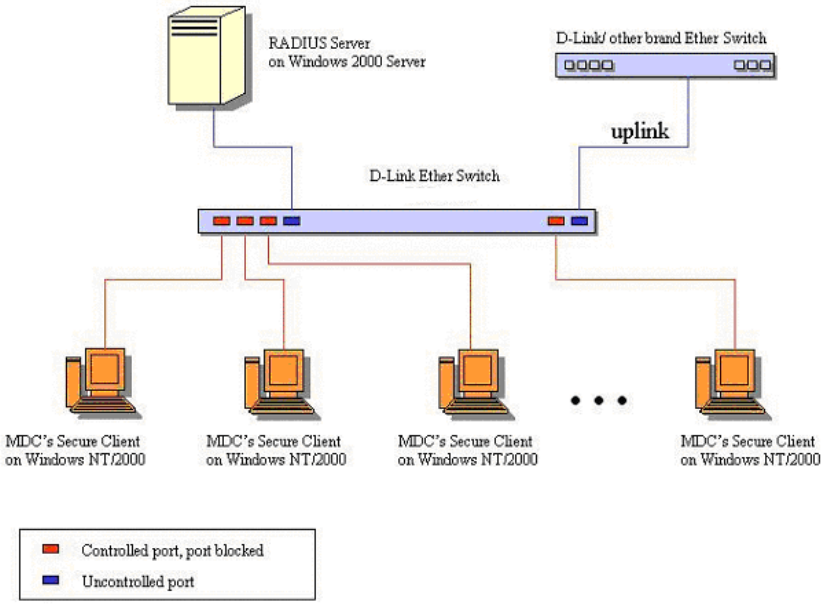



**Figure 6- 55. Typical 802.1x Configuration Prior to User Authentication**

Once the user is authenticated, the Switch unblocks the port that is connected to the user as shown in the next figure.

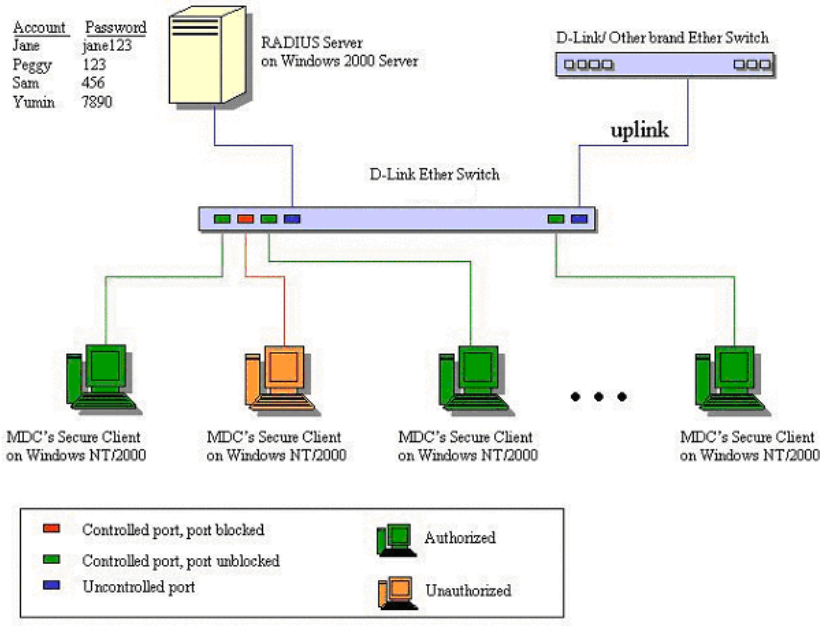



**Figure 6- 56. Typical 802.1x Configuration with User Authentication**

The user's information, including account number, password, and configuration details such as IP address and billing information, is stored in a centralized RADIUS server.

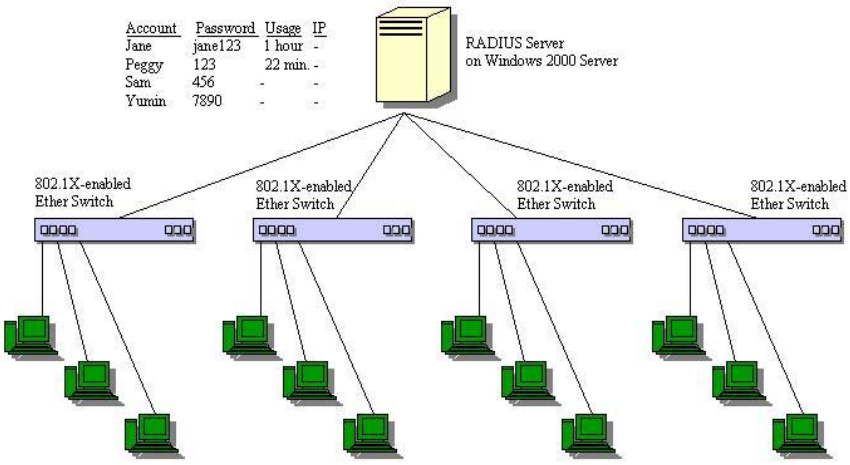



**Figure 6- 57. Typical Configuration with 802.1x Fully Implemented**

| State Machine Name |
|---|
| Port Timers state machine |
| Authenticator PAE state machine |
| The Authenticator Key Transmit state machine |
| Reauthentication Timer state machine |
| Backend Authentication state machine |
| Controlled Directions state machine |
| The Key Receive state machine |

**Table 6- 2. Conformance to IEEE 802.1x Standards**

The DES-3550 implements the server-side of the **IEEE 802.1x Port-based Network Access Control.** This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the Switch that a user or network device must meet before allowing that port to forward or receive frames.

IEEE 802.1x operation must be enabled on the Switch before it will function. This is done using the **802.1x State** window. 802.1x settings can be configured before being enabled on the Switch.

## Configure Authenticator

To configure the **802.1X Authenticator Settings**, click **PAE Access Entity > Configure Authenticator:**

802.1X Authenticator Settings

| Port | AdminCtrlDir | OperCtrlDir | Port Ctrl | TxPeriod | Quiet Period | Supp-Timeout | Server-Timeout | MaxReq | ReAuth Period | ReAuth Enabled |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 2 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 3 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 4 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 5 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 6 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 7 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 8 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 9 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 10 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 11 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 12 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 13 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 14 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 15 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 16 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 17 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 18 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 19 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 20 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 21 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 22 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 23 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 24 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 25 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 26 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 27 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 28 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 29 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 30 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 31 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 32 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 33 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 34 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 35 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 36 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 37 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 38 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 39 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 40 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 41 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 42 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 43 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 44 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 45 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 46 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 47 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 48 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 49 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |
| 50 | both | both | auto | 30 | 60 | 30 | 30 | 2 | 3600 | no |

**Figure 6- 58. 802.1X Authenticator Settings window**

To configure the settings by port, click on the hyperlinked port number under the **Port** heading, which will display the following table to configure:

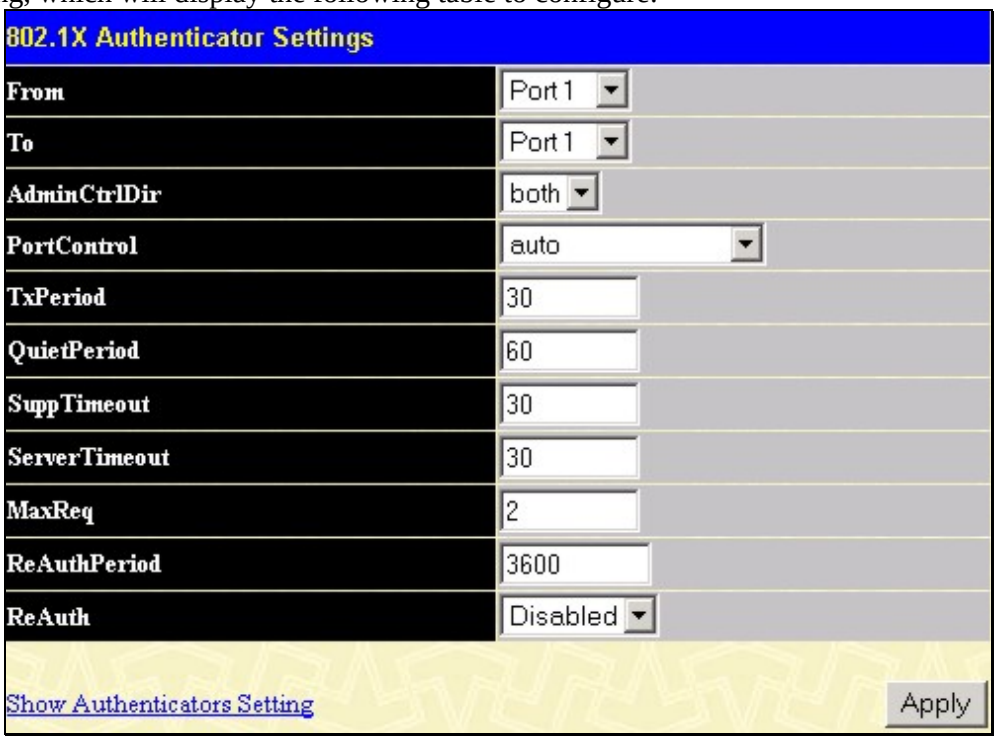



**Figure 6- 59. 802.1X Authenticator Settings - Modify**

This screen allows you to set the following features:

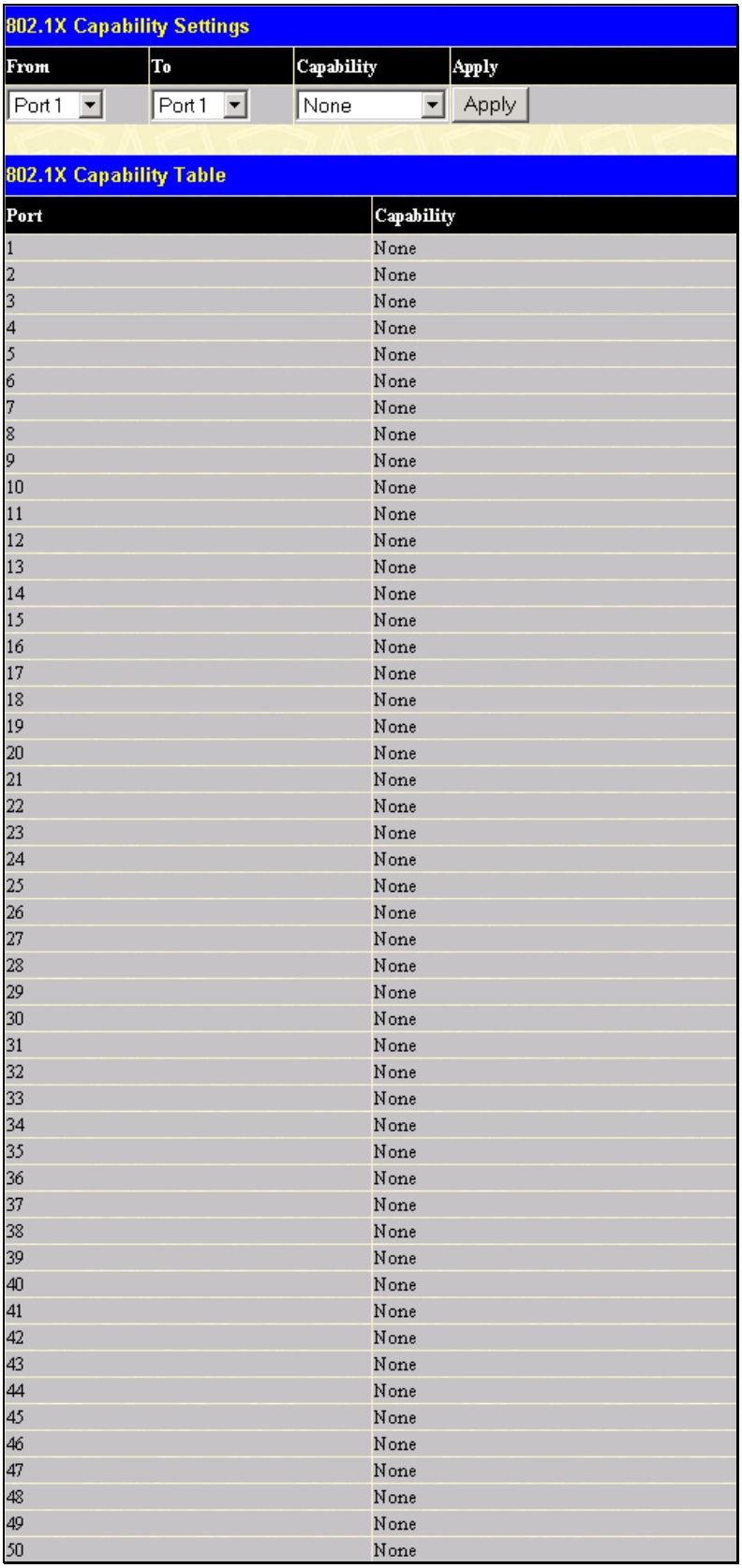
| Parameter | Description |
|---|---|
| **Configure Port from [ ] to [ ]** | Enter the port or ports to be set. |
| **AdmCtrlDir:<*both*>** | Sets the administrative-controlled direction to either *in* or *both*. If *in* is selected, control is only exerted over incoming traffic through the port you selected in the first field. If *both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field. |
| **PortControl:<** *forceUnauthorized* **>** | This allows you to control the port authorization state. Select *forceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *forceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface. The third option is *auto*. This enables 802.1X and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. |

| | |
|---|---|
| **TxPeriod:[*30* ]** | This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. |
| **QuietPeriod:[*60* ]** | This allows you to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. |
| **SuppTimeout:[*30* ]** | This value determines timeout conditions in the exchanges between the Authenticator and the client. |
| **ServerTimeout:[*30* ]** | This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. |
| **MaxReq:[*2* ]** | The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. |
| **ReAuthPeriod:[*3600* ]** | A constant that defines a nonzero number of seconds between periodic reauthentication of the client. |
| **ReAuth:<*Disabled*>** | Determines whether regular reauthentication will take place on this port. |

Click *Apply* to implement your configuration changes. To view configurations for the **802.1X Authenticator Settings** on a port-by-port basis, see the **802.1X Authenticator Settings** table.

## Port Capability Settings

Existing 802.1x port settings are displayed and can be configured using the window below.
Click **Port Capability Settings** on the **PAE Access Entity** folder to open the **802.1X Capability Settings** window***:***



802.1X Capability Settings

| From | To | Capability | Apply |
|---|---|---|---|
| Port 1 | Port 1 | None | Apply |

802.1X Capability Table

| Port | Capability |
|---|---|
| 1 | None |
| 2 | None |
| 3 | None |
| 4 | None |
| 5 | None |
| 6 | None |
| 7 | None |
| 8 | None |
| 9 | None |
| 10 | None |
| 11 | None |
| 12 | None |
| 13 | None |
| 14 | None |
| 15 | None |
| 16 | None |
| 17 | None |
| 18 | None |
| 19 | None |
| 20 | None |
| 21 | None |
| 22 | None |
| 23 | None |
| 24 | None |
| 25 | None |
| 26 | None |
| 27 | None |
| 28 | None |
| 29 | None |
| 30 | None |
| 31 | None |
| 32 | None |
| 33 | None |
| 34 | None |
| 35 | None |
| 36 | None |
| 37 | None |
| 38 | None |
| 39 | None |
| 40 | None |
| 41 | None |
| 42 | None |
| 43 | None |
| 44 | None |
| 45 | None |
| 46 | None |
| 47 | None |
| 48 | None |
| 49 | None |
| 50 | None |

**Figure 6- 60. 802.1x Capability Settings and Table window**

To set up the Switch's 802.1x port-based authentication, select which ports are to be configured in the *From* and *To* fields. Next, enable the ports by selecting *Authenticator* from the drop-down menu under **Capability**. Click *Apply* to make your change take effect.
Configure the following 802.1x capability settings:

| Parameter | Description |
|---|---|
| **From** and **To** | Ports being configured for 802.1x settings. |
| **Capability** | Two role choices can be selected:<br>*Authenticator* – A user must pass the authentication process to gain access to the network.<br>*None* – The port is not controlled by the 802.1x functions. |

## Initializing Ports

Existing 802.1x port settings are displayed and can be configured using the window below. Click **Initialize Port(s)** on the **PAE Access Entity** folder on the **Configuration** menu to open the **802.1x Port Initial** window:

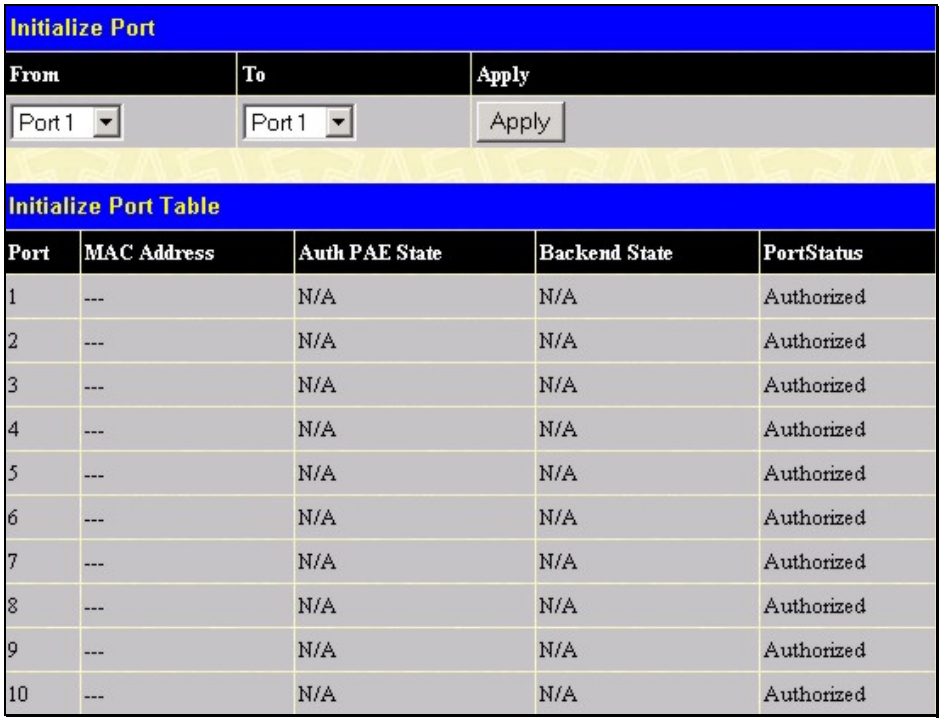



**Figure 6- 61. 802.1x Port Initial and Port Authentication state window**

This window allows you to initialize a port or group of ports. The **Initialize Port Table** in the bottom half of the window displays the current status of the port(s) once you have clicked *Apply*.
This window displays the following information:

| Parameter | Description |
|---|---|

| | |
|---|---|
| **From and To** | Select ports to be initialized. |
| **Port** | A read only field indicating a port on the Switch. |
| **MAC Address** | The MAC address of the Switch connected to the corresponding port, if any. |
| **Auth PAE State** | The Authenticator PAE State will display one of the following: *Initialize*, *Disconnected*, *Connecting*, *Authenticating*, *Authenticated*, *Aborting*, *Held*, *ForceAuth*, *ForceUnauth*, and *N/A*. |
| **Backend State** | The Backend Authentication State will display one of the following: *Request*, *Response*, *Success*, *Fail*, *Timeout*, *Idle*, *Initialize,* and *N/A.* |
| **Port Status** | The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*. |

**Note**: The user must first globally enable 802.1X in the **Advanced Settings** window in the **Configuration** folder before initializing ports. Information in the **Initialize Ports Table** cannot be viewed before enabling 802.1X.

## Reauthenticate Port(s)

This window allows you to reauthenticate a port or group of ports by choosing a port or group of ports by using the pull down menus **From** and **To** and clicking *Apply*. The **Reauthenticate Port Table** displays the current status of the reauthenticated port(s) once you have clicked *Apply*.

Click **Reauthenticate Port(s)** on the **PAE Access Entity** folder on the **Configuration** menu to open the **Reauthenticate Port(s)** window:

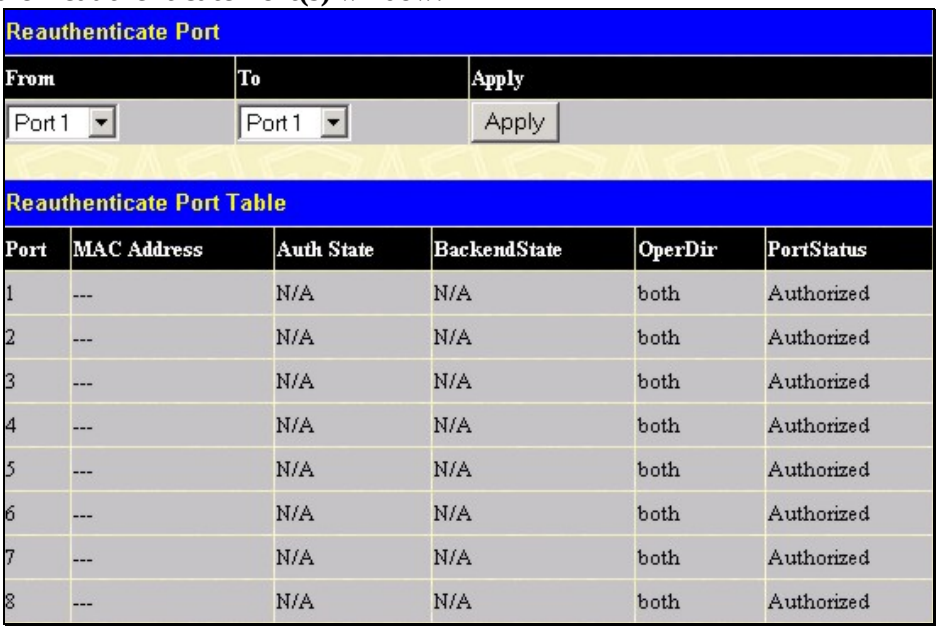



**Figure 6- 62. Reauthenticate Port and Reauthenticate Port Table window**

This window displays the following information:

| Parameter | Description |
|---|---|

| | |
|---|---|
| **Port** | The port number. |
| **MAC Address** | Displays the physical address of the Switch where the port resides. |
| **Auth State** | The Authenticator State will display one of the following: *Initialize*, *Disconnected*, *Connecting*, *Authenticating*, *Authenticated*, *Aborting*, *Held*, *ForceAuth*, ForceUnauth, and *N/A*. |
| **BackendState** | The Backend State will display one of the following: *Request*, *Response*, *Success*, *Fail*, *Timeout*, *Idle*, *Initialize,* and *N/A.* |
| **OpenDir** | Operational Controlled Directions are *both* and *in*. |
| **PortStatus** | The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*. |

## RADIUS Server

The RADIUS feature of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker. The Web Manager offers three windows.

Click the **Radius Server folder** on the **Configuration** menu, and then click the **Authentic Radius Server** link to open the **Authentic Radius Server Setting** window:

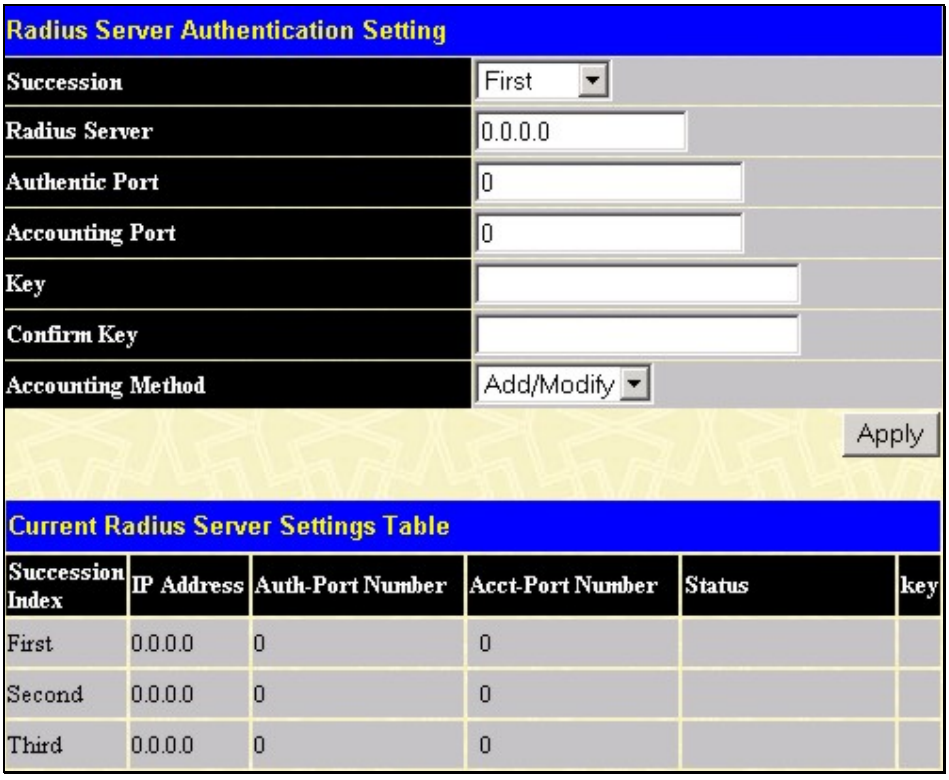



**Figure 6- 63. Authentic Radius Server Setting and Current Radius Server(s) Settings Table window**

This window displays the following information:

| Parameter | Description |
|---|---|

| | |
|---|---|
| **Succession <***First***>** | Choose the desired RADIUS server to configure: *First*, *Second,* or *Third*. |
| **Radius Server <***10.53.13.94***>** | Set the RADIUS server IP. |
| **Authentic Port <***1812***>** | Set the RADIUS authentic server(s) UDP port. The default is *1812*. |
| **Accounting Port <***1813***>** | Set the RADIUS account server(s) UDP port. The default is *1813*. |
| **Key** | Set the key the same as that of the RADIUS server. |
| **Confirm Key** | Confirm the shared key is the same as that of the RADIUS server. |
| **Accounting Method** | This allows you to *Add/Modify* or *Delete* the RADIUS Server. |

Section 7

# Management

***Security IP***
***User Accounts***
***Access Authentication Control (TACACS)***
***SNMP V3***

The following section will aid the user in configuring security functions for the Switch. The Switch includes various functions for security, including TACACS, Security IPs, and SNMP, all discussed in detail in the following section.

## Security IP

Go to the **Management** folder and click on the **Security IP** link; the following screen will appear.

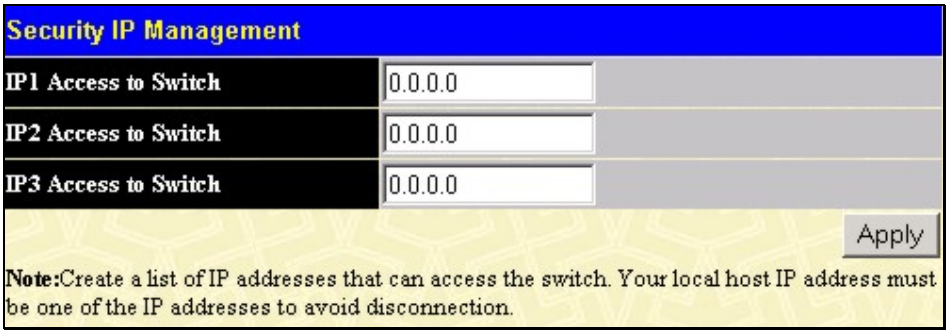

Security IP Management
IP1 Access to Switch
0.0.0.0
IP2 Access to Switch
0.0.0.0
IP3 Access to Switch
0.0.0.0
Apply
Note:Create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.

**Figure 7- 1. Security IP Management Setup**

Use the **Security IP Management** to permit remote stations to manage the Switch. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the Web manager or Telnet session. To define a management station IP setting, type in the IP address and click on the *Apply* button.

### User Accounts

Use the **User Accounts Management** window to control user privileges. To view existing **User Accounts**, open the **Security Management** folder and click on the **User Accounts** link. This will open the **User Account Management** page, as shown below.

**Figure 7- 2. User Accounts Management Table**

To add a new user, click on the *Add* button. To modify or delete an existing user, click on the *Modify* button for that user.

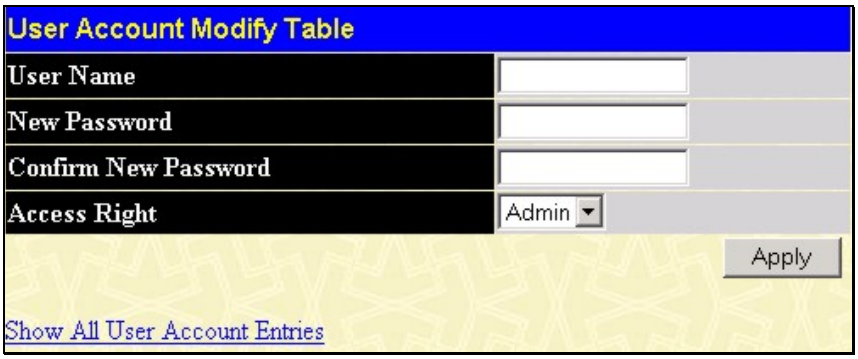



**Figure 7- 3. User Accounts Modify Table - Add**

Add a new user by typing in a **User Name** and **New Password** and retype the same password in the **Confirm New Password**. Choose the level of privilege (**Admin** or **User**) from the **Access Right** drop-down menu.

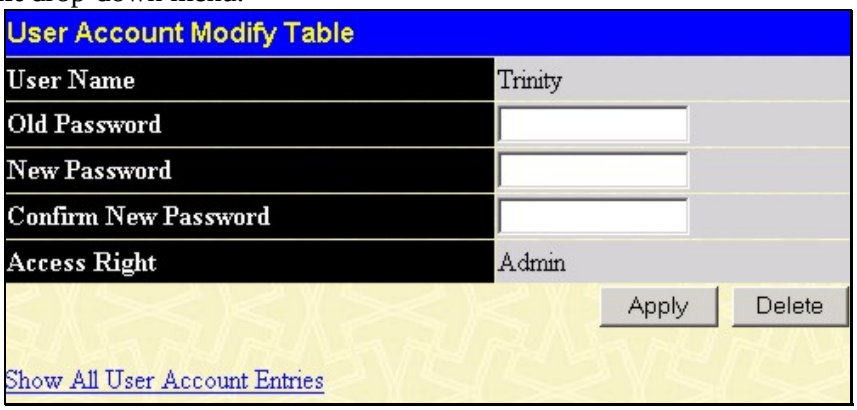



**Figure 7- 4. Modify User Accounts**

Modify or delete an existing user account in the **User Account Modify Table**. To delete the user account, click on the *Delete* button. To change the password, type in the **New Password** and retype it in the **Confirm New Password** entry field. Choose the level of privilege (**Admin** or **User**) from the **Access Right** drop-down menu.

## Admin and User Privileges

There are two levels of user privileges: **Admin** and **User**. Some menu selections available to users with **Admin** privileges may not be available to those with **User** privileges.
The following table summarizes the **Admin** and **User** privileges:

| Management | Admin | User |
|---|---|---|
| **Configuration** | Yes | Read Only |
| **Network Monitoring** | Yes | Read Only |
| **Community Strings and Trap Stations** | Yes | Read Only |
| **Update Firmware and Configuration Files** | Yes | No |
| **System Utilities** | Yes | No |
| **Factory Reset** | Yes | No |

| User Account Management | | |
|---|---|---|
| **Add/Update/Delete User Accounts** | Yes | No |
| **View User Accounts** | Yes | No |

**Admin and User Privileges**

After establishing a **User Account** with *Admin*-level privileges, be sure to save the changes by opening the **Maintenance** folder, opening the **Save Changes** window and clicking the *Save Configuration* button.

# Access Authentication Control

The TACACS / XTACACS / TACACS+ commands let you secure access to the Switch using the TACACS / XTACACS / TACACS+ protocols. When a user logs in to the Switch or tries to access the administrator level privelege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ authentication is enabled on the Switch, it will contact a TACACS / XTACACS / TACACS+ server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

- TACACS (Terminal Access Controller Access Control System) — Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- Extended TACACS (XTACACS) — An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- TACACS+ (Terminal Access Controller Access Control System plus) — Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery.

In order for the TACACS / XTACACS / TACACS+ security function to work properly, a TACACS / XTACACS / TACACS+ server must be configured on a device other than the Switch, called an *Authentication Server Host*, and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS / XTACACS / TACACS+ server to verify, and the server will respond with one of three messages:

- The server verifies the username and password, and the user is granted normal user privileges on the Switch.
- The server will not accept the username and password and the user is denied access to the Switch.
- The server does not respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has three built-in *Authentication Server Groups*, one for each of the TACACS, XTACACS, and TACACS+ protocols. These built-in *Authentication Server Groups* are used to authenticate users trying to access the Switch. The users will set *Authentication Server*

*Hosts* in a preferable order in the built-in *Authentication Server Groups* and when a user tries to gain access to the Switch, the Switch will ask the first *Authentication Server Hosts* for authentication. If no authentication is made, the second *server host* in the list will be queried, and so on. The built-in *Authentication Server Groups* can only have hosts that are running the specified protocol. For example, the TACACS *Authentication Server Groups* can only have TACACS *Authentication Server Hosts.*

The administrator for the Switch may set up five different authentication techniques per user-defined *method list* (TACACS / XTACACS / TACACS+ / local / none) for authentication. These techniques will be listed in a preferred order, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its *Authentication Server Hosts* and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that users granted access to the Switch will be granted normal user privileges on the Switch. To gain access to administrator level privileges, the user must access the **Enable Admin** window and then enter a previously configured password, set by the administrator of the Switch.

**NOTE:** TACACS, XTACACS, and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must the host server.)

## Policy & Parameters

This command will enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the **Login Method List** and choose a technique for user authentication upon login.

To access the following window, click **Management > Access Authentication Control > Policy & Parameters:**

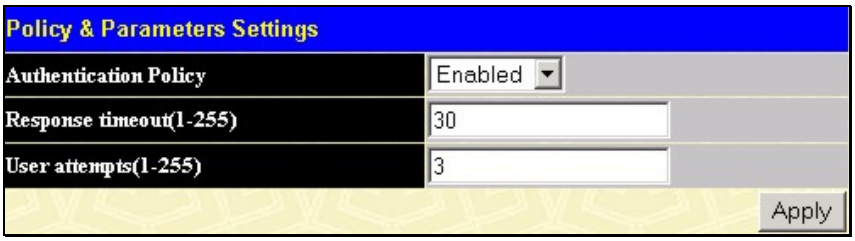



**Figure 7- 5. Policy & Parameters Settings window**

The following parameters can be set:

| Parameters | Description |
|---|---|
| **Authentication Policy** | Use the pull down menu to enable or disable the *Authentication Policy* on the Switch. |
| **Response Timeout(1-255)** | This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between 1 and 255 seconds. The default setting is 30 seconds. |
| **User Attempts(1-255)** | This command will configure the maximum number of times the |

| | |
|---|---|
| | Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from 1 to 255. The default setting is 3. |

Click *Apply* to implement changes made.

## Application's Authentication Settings

This window is used to configure switch configuration applications (console, telnet, web) for login at the user level and at the administration level (*Enable Admin*) utilizing a previously configured method list.

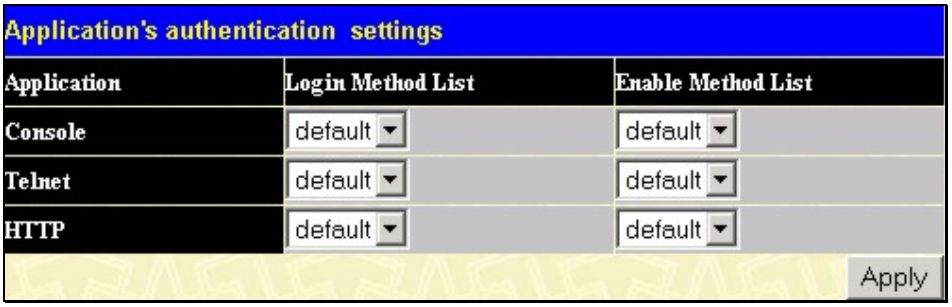



**Figure 7- 6. Application's Authentication Settings**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **Application** | Lists the configuration applications on the Switch. The user may configure the *Login Method List* and *Enable Method List* for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, and the WEB (HTTP) application. |
| **Login Method List** | Using the pull down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the *Login Method Lists* window, in this section, for more information |
| **Enable Method List** | Using the pull down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the *Enable Method Lists* window, in this section, for more information |

Click *Apply* to implement changes made.

## Authentication Server Group Settings

This window will allow users to set up *Authentication Server Groups* on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+ server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in **Authentication Server Groups** that cannot be removed but can be modified. Up to eight (8) authentication server hosts may be added to any particular group.

To view the following window, click **Management > Access Authentication Control > Authentication Server Group:**

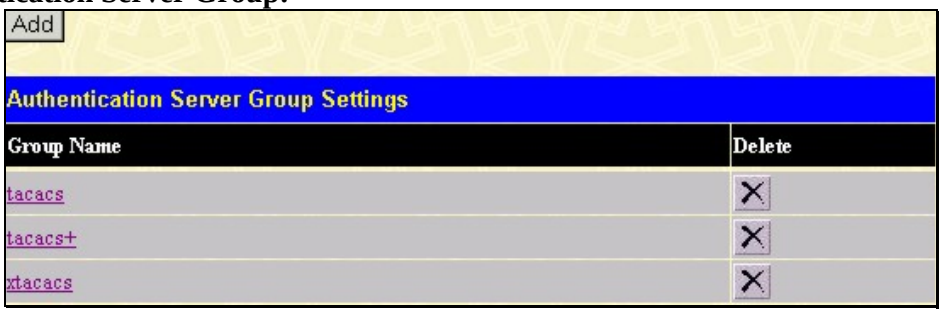



**Figure 7- 7. Authentication Server Group Settings window**

This screen displays the *Authentication Server Groups* on the Switch. The Switch has three built-in **Authentication Server Groups** that cannot be removed but can be modified. To modify a particular group, click its hyperlinked **Group Name**, which will then display the following window.

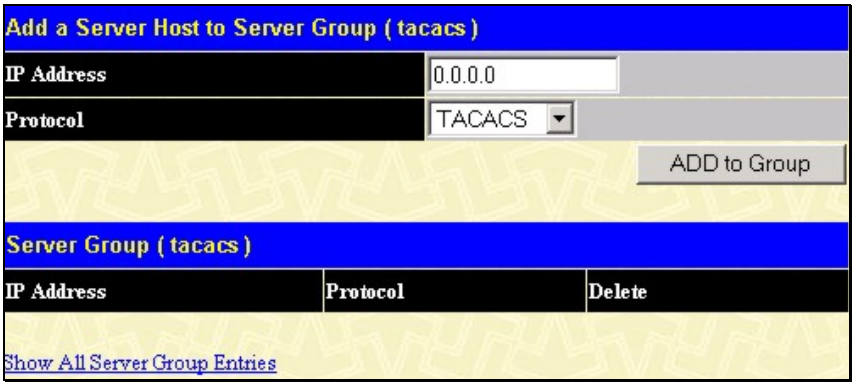



**Figure 7- 8. Add a Server Host to Server Group (tacacs) window.**

To add an *Authentication Server Host* to the list, enter its IP address in the IP Address field, choose the protocol associated with the IP address of the *Authentication Server Host*, and click *ADD to Group* to add this *Authentication Server Host* to the group.

**NOTE:** The user must configure *Authentication Server Hosts* using the *Authentication Server Hosts* window before adding hosts to the list. *Authentication Server Hosts* must be configured for their specific protocol on a remote centralized server before this function can work properly.

**NOTE:** The three built-in server groups on the Switch can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ protocols are separate entities and are not compatible with each other.

## Authentication Server Hosts

This window will set user-defined *Authentication Server Hosts* for the TACACS/XTACACS/TACACS+ security protocols on the Switch. When a user attempts to access the Switch with *Authentication Policy* enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+ server host on a remote host. The TACACS/XTACACS/TACACS+ server host will then verify or deny the request and return the

appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

To view the following window, click **Management > Access Authentication Control > Authentication Server Host:**

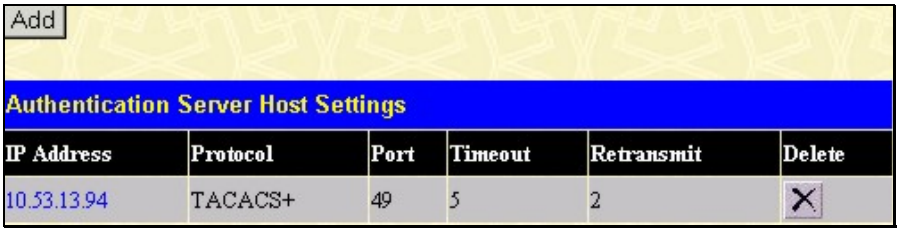



**Figure 7- 9. Authentication Server Host Settings window**

To add an *Authentication Server Host,* click the *Add* button, revealing the following window:

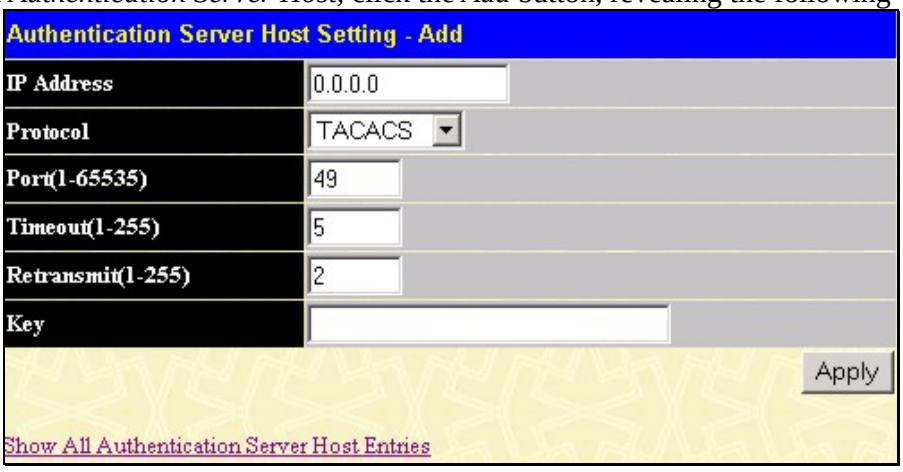



**Figure 7- 10. Authentication Server Host Settings window - Add**

Configure the following parameters to add an *Authentication Server Host*:

| Parameter | Description |
|---|---|
| **IP Address** | The IP address of the remote server host the user wishes to add. |
| **Protocol** | The protocol used by the server host. The user may choose one of the following:<br>**TACACS** – Enter this parameter if the server host utilizes the tacacs protocol.<br>**XTACACS** - Enter this parameter if the server host utilizes the xtacacs protocol.<br>**TACACS+** - Enter this parameter if the server host utilizes the tacacs+ protocol. |
| **Port(1-65535)** | Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers but the user may set a unique port number for higher security. |
| **Timeout(1-255)** | Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds. |

| | |
|---|---|
| **Retransmit(1-255)** | Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond. |
| **Key** | Authentication key to be shared with a configured TACACS+ server only. Specify an alphanumeric string up to 254 characters. |

Click *Apply* to add the server host.

**NOTE:** More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other.

## Login Method Lists

This command will configure a user-defined or default *Login Method List* of authentication techniques for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example *TACACS – XTACACS– local,* the Switch will send an authentication request to the first *TACACS* host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, *XTACACS*. If no authentication takes place using the *XTACACS* list, the *local* account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch.
Successful login using any of these techniques will give the user a "user" privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must use the *Enable Admin* window, in which the user must enter a previously configured password, set by the administrator. *(See the **Enable Admin** part of this section for more detailed information concerning the **Enable Admin** command.)*

To view the following screen click **Management > Access Authentication Control > Login Method Lists:**

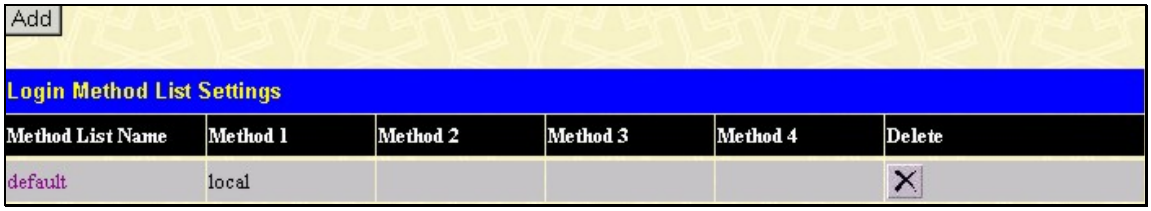



**Figure 7- 11. Login Method Lists Settings window**

The Switch contains one *Method List* that is set and cannot be removed, yet can be modified.

To delete a **Login Method List** defined by the user, click the ✕ under the **Delete** heading corresponding to the entry desired to be deleted. To modify a **Login Method List**, click on its hyperlinked **Method List Name**. To configure a Method List, click the *Add* button.

Both actions will result in the same screen to configure:

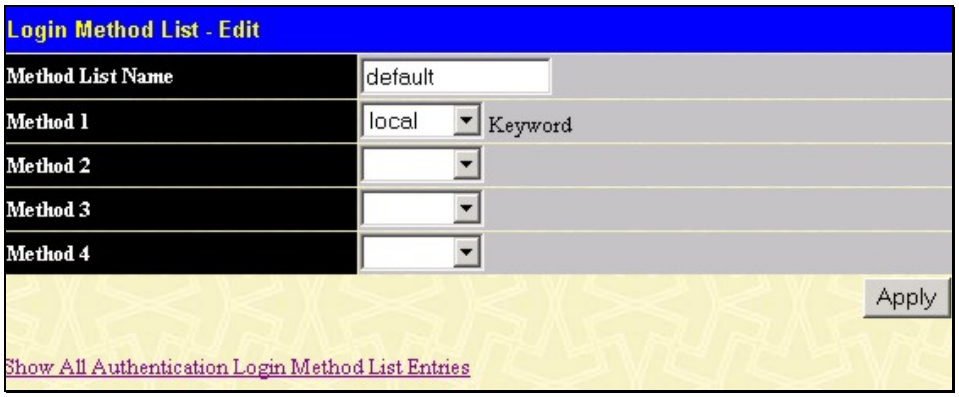



**Figure 7- 12. Login Method List –Edit (default)**

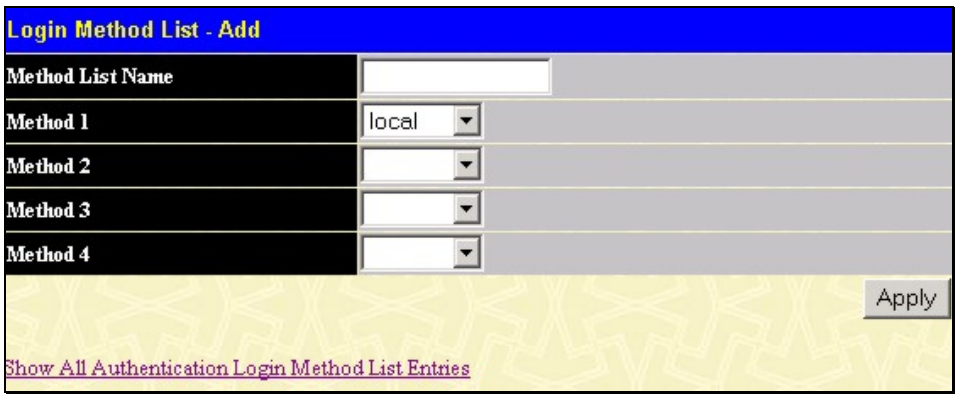



**Figure 7- 13. Login Method List – Add**

To define a **Login Method List**, set the following parameters and click *Apply*:

| Parameter | Description |
|---|---|
| **Method List Name** | Enter a method list name defined by the user of up to 15 characters. |
| **Method 1, 2, 3, 4** | The user may add one, or a combination of up to four (4) of the following authentication methods to this method list:<br>tacacs – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from a remote tacacs server.<br>xtacacs – Adding this parameter will require the user to be authenticated using the x*tacacs* protocol from a remote xtacacs server.<br>tacacs+ – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from a remote tacacs server.<br>server_group - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.<br>local - Adding this parameter will require the user to be authenticated using the local *user account* database on the Switch.<br>none – Adding this parameter will require no authentication to access the Switch. |

## Enable Method Lists

This window is used to set up Method Lists to promote users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) **Enable Method Lists** can be implemented on the Switch, one of which is a default *Enable Method List.* This default *Enable Method List* cannot be deleted but can be configured.
The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *TACACS – XTACACS – Local Enable,* the Switch will send an authentication request to the first *TACACS* host in the server group. If no verification is found, the Switch will send an authentication request to the second *TACACS* host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, *XTACACS*. If no authentication takes place using the *XTACACS* list, the *Local Enable* password set in the Switch is used to authenticate the user.
Successful authentication using any of these methods will give the user an "Admin" privilege.

**NOTE:** To set the *Local Enable Password*, see the next section, entitled **Local Enable Password.**

To view the following table, click **Management > Access Authentication Control > Enable Method Lists**:

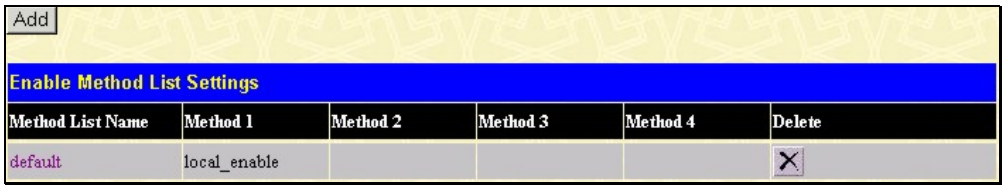



**Figure 7- 14. Enable Method List Settings window.**

To delete an **Enable Method List** defined by the user, click the under the **Delete** heading corresponding to the entry desired to be deleted. To modify an **Enable Method List**, click on its hyperlinked **Enable Method List Name**. To configure a Method List, click the *Add* button.

Both actions will result in the same screen to configure:

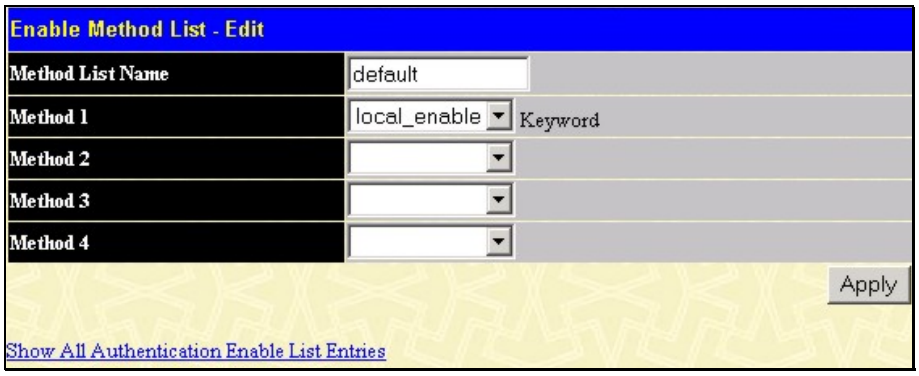



**Figure 7- 15. Enable Method List – Edit window**

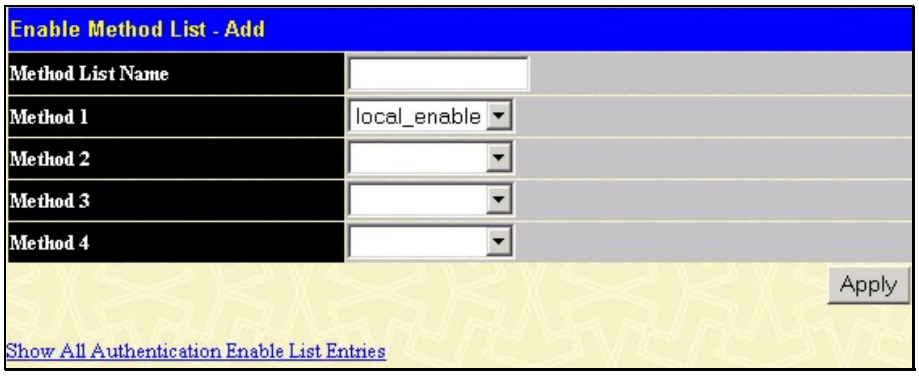



**Figure 7- 16. Enable Method List – Add window**

To define an **Enable Login Method List**, set the following parameters and click *Apply*:

| Parameter | Description |
|---|---|
| **Method List Name** | Enter a method list name defined by the user of up to 15 characters. |
| **Method 1, 2, 3, 4** | The user may add one, or a combination of up to four (4) of the following authentication methods to this method list:<br>local_enable - Adding this parameter will require the user to be authenticated using the *local enable password* database on the Switch. The *local enable password* must be set by the user in the next section entitled **Local Enable Password**.<br>none – Adding this parameter will require no authentication to access the Switch.<br>tacacs – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from a remote tacacs server.<br>xtacacs – Adding this parameter will require the user to be authenticated using the x*tacacs* protocol from a remote xtacacs server.<br>tacacs+ – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from a remote tacacs server.<br>server_group - Adding a previously configured server group will require the user to be authenticated using a user-defined server group previously configured on the Switch. |

## Local Enable Password

This window will configure the locally enabled password for the *Enable Admin* command. When a user chooses the "*Local_Enable*" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.
To view the following window, click **Management > Access Authentication Control > Local Enable Password**:

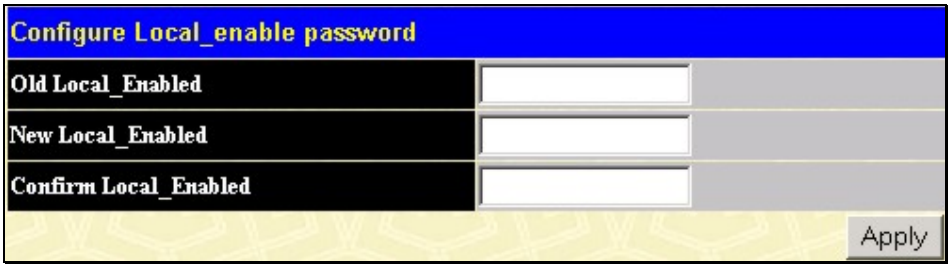



**Figure 7- 17. Configure Local Enable Password window**

To set the *Local Enable Password*, set the following parameters and click *Apply*.

| Parameter | Description |
|---|---|
| **Old Local Enabled** | If a password was previously configured for this entry, enter it here in order to change it to a new password. |
| **New Local Enabled** | Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters. |
| **Confirm Local Enabled** | Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message. |

## Enable Admin

This window is for users who have logged on to the Switch on the normal user level, and wish to be promoted to the administrator level. After logging on to the Switch, users will have only user level privileges. To gain access to administrator level privileges, the user will open this window and will have to enter an authentication password. Possible authentication methods for this function include TACACS/XTACACS/TACACS+, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host, which has the username "enable", and a password configured by the administrator that will support the "enable" function. This function becomes inoperable when the authentication policy is disabled.

To view the following window, click Management > Access Authentication Control > Enable Admin:

Enable Admin
Click "Enable Admin" button will let user input the new password to upgrade this web management to "Admin" level.
If the password is incorrect for 3 times, web management will stay at the login page and wait for user to login again.
Enable Admin

**Figure 7- 18. Enable Admin Screen**

When this screen appears, click the *Enable Admin* button revealing a window for the user to enter authentication (password, username), as seen below. A successful entry will promote the user to Administrator level privileges on the Switch.

**Figure 7- 19. Enter Network Password window**

# SNMP

## SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance, and detect potential problems in the switch, switch group, or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The DES-3550 supports the SNMP versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).
The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

**public** - Allows authorized management stations to retrieve MIB objects.

**private** - Allows authorized management stations to retrieve and modify MIB objects.

SNMP v.3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.
The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMP v.1 while assigning a higher level of security to another group, granting read/write privileges using SNMP v.3.
Using SNMP v.3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMP v.3 in that SNMP messages may be encrypted.

### Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change, and Broadcast\Multicast Storm.

### MIBs

Management and counter information are stored by the Switch in the Management Information Base (MIB). The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. The proprietary MIB may also be retrieved by specifying the MIB Object Identifier. MIB values can be either read-only or read-write.

The DES-3550 incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.
The DES-3550 supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP settings are configured using the menus located on the SNMP V3 folder of the web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the Management Station IP Address menu.

## SNMP User Table

The **SNMP User Table** displays all of the SNMP User's currently configured on the Switch. In the **SNMP V3** folder, click on the **SNMP User Table** link. This will open the **SNMP User Table**, as shown below.

**Figure 7- 20. SNMP User Table**

To delete an existing SNMP User Table entry, click the ✕ below the **Delete** heading corresponding to the entry you wish to delete.
To display the detailed entry for a given user, click on the hyperlinked **User Name**. This will open the **SNMP User Table Display** page, as shown below.

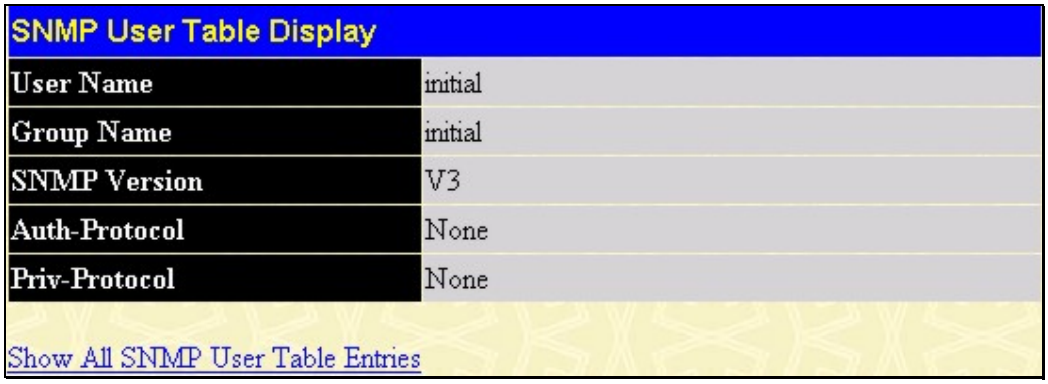



**Figure 7- 21. SNMP User Table Display**

The following parameters are displayed:

| Parameter | Description |
|---|---|
| **User Name** | An alphanumeric string of up to 32 characters. This is used to identify the SNMP users. |
| **Group Name** | This name is used to specify the SNMP group created can request SNMP messages. |
| **SNMP Version** | **V1** – Indicates that SNMP version 1 will be used.<br>**V2** – Indicates that SNMP version 2 will be used.<br>**V3** – Indicates that SNMP version 3 will be used. |

| | |
|---|---|
| **Auth-Protocol** | **None –** Indicates that no authorization protocol is in use.<br>**MD5** – Indicates that the HMAC-MD5-96 authentication level will be used.<br>**SHA** – Indicates that the HMAC-SHA authentication protocol will be used. |
| **Priv-Protocol** | **None –** Indicates that no authorization protocol is in use.<br>**DES –** Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard. |

To return to the **SNMP User Table**, click the Show All SNMP User Table Entries link.

To add a new entry to the **SNMP User Table Configuration**, click on the *Add* button on the **SNMP User Table** page. This will open the **SNMP User Table Configuration** page, as shown below.

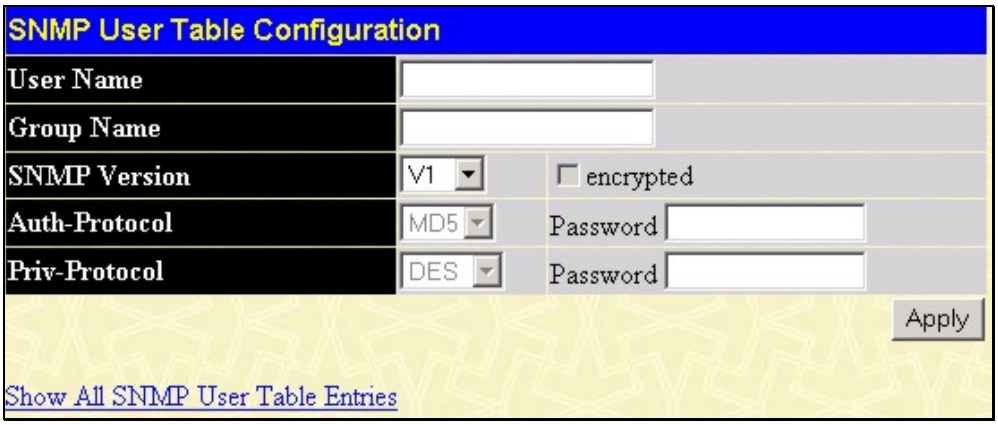



**Figure 7- 22. SNMP User Table Configuration**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **User Name** | An alphanumeric string of up to 32 characters. This is used to identify the SNMP users. |
| **Group Name** | This name is used to specify the SNMP group created can request SNMP messages. |
| **SNMP Version** | **V1** – Specifies that SNMP version 1 will be used.<br>**V2c** – Specifies that SNMP version 2 will be used.<br>**V3** – Specifies that SNMP version 3 will be used. |
| **Auth-Protocol** | **MD5** – Specifies that the HMAC-MD5-96 authentication level will be used.<br>**SHA** – Specifies that the HMAC-SHA authentication protocol will be used. |
| **Priv-Protocol** | **None –** Specifies that no authorization protocol is in use.<br>**DES –** Specifies that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. |

| | |
|---|---|
| **encrypted** | Checking the corresponding box will enable encryption for SNMP V3 and is only operable in SNMP V3 mode. |

To implement the changes, click *Apply*. To return to the **SNMP User Table**, click the Show All SNMP User Table Entries link.

## SNMP View Table

The **SNMP View Table** is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager. To view the **SNMP View Table**, open the **SNMP V3** folder and click the **SNMP View Table** entry. The following screen should appear:

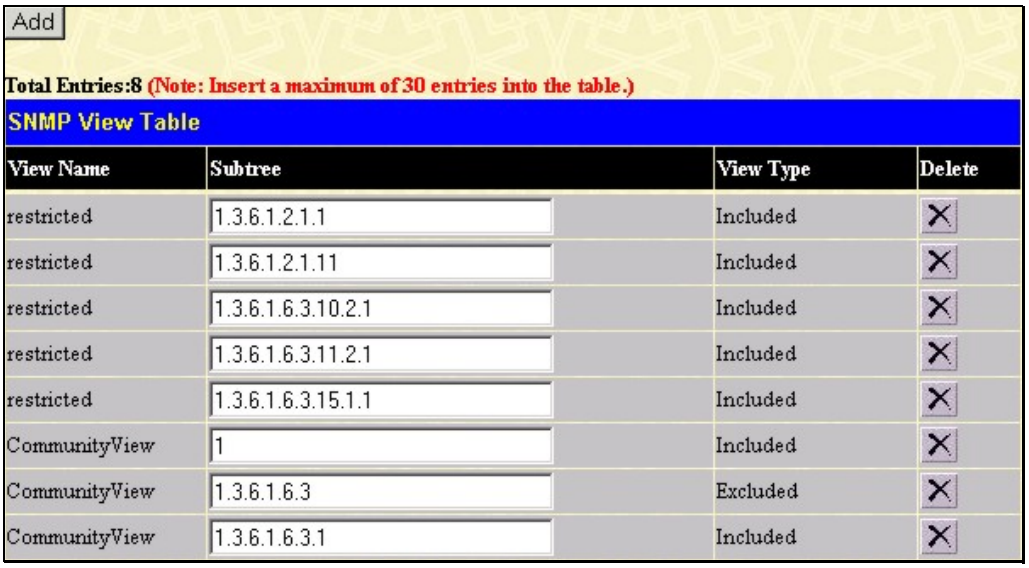



**Figure 7- 23. SNMP View Table**

To delete an existing **SNMP View Table** entry, click the ✕ in the **Delete** column corresponding to the entry you wish to delete. To create a new entry, click the *Add* button; a separate menu will appear.

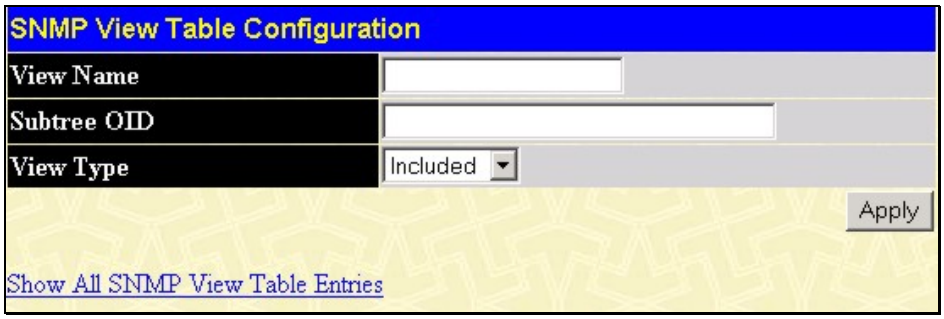



**Figure 7- 24. SNMP View Table Configuration**

The SNMP Group created with this table maps SNMP users (identified in the **SNMP User Table**) to the views created in the previous menu.
The following parameters can be set:

| Parameter | Description |
|---|---|

| | |
|---|---|
| **View Name** | Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created. |
| **Subtree OID** | Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager. |
| **View Type** | Select **Included** to include this object in the list of objects that an SNMP manager can access. Select **Excluded** to exclude this object from the list of objects that an SNMP manager can access. |

To implement your new settings, click *Apply*. To return to the **SNMP View Table**, click the Show All SNMP View Table Entries link.

## SNMP Group Table

A SNMP Group created with this table maps SNMP users (identified in the **SNMP User Table**) to the views created in the previous menu. To view the **SNMP Group Table**, open the **SNMP V3** folder and click the **SNMP Group Table** entry. The following screen should appear:

Add

Total Entries:9 (Note: Insert a maximum of 30 entries into the table.)

SNMP Group Table

| Group Name | Security Model | Security Level | Delete |
|---|---|---|---|
| public | SNMPv1 | NoAuthNoPriv | |
| public | SNMPv2 | NoAuthNoPriv | |
| initial | SNMPv3 | NoAuthNoPriv | |
| private | SNMPv1 | NoAuthNoPriv | |
| private | SNMPv2 | NoAuthNoPriv | |
| ReadGroup | SNMPv1 | NoAuthNoPriv | |
| ReadGroup | SNMPv2 | NoAuthNoPriv | |
| WriteGroup | SNMPv1 | NoAuthNoPriv | |
| WriteGroup | SNMPv2 | NoAuthNoPriv | |

**Figure 7- 25. SNMP Group Table**

To delete an existing **SNMP Group Table** entry, click the corresponding ✕ under the **Delete** heading.
To display the current settings for an existing **SNMP Group Table** entry, click the blue hyperlink for the entry under the *Group Name*.

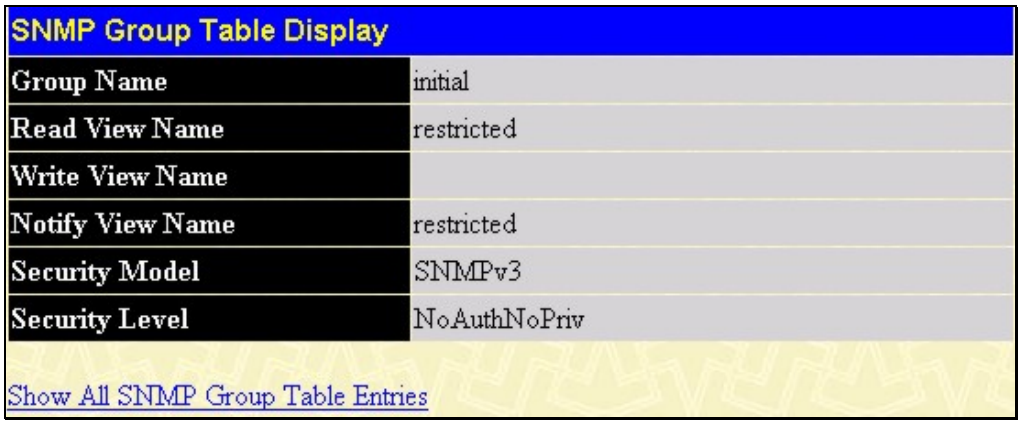



**Figure 7- 26. SNMP Group Table Display**

To add a new entry to the Switch's **SNMP Group Table**, click the *Add* button in the upper left-hand corner of the **SNMP Group Table** page. This will open the **SNMP Group Table Configuration** page, as shown below.

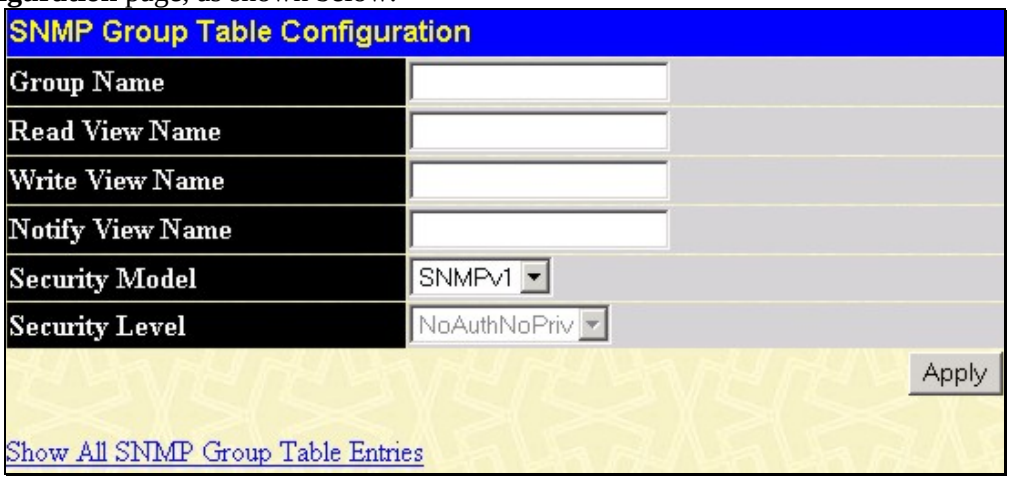



**Figure 5- 3. SNMP Group Table Configuration**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **Group Name** | Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users. |
| **Read View Name** | This name is used to specify that the SNMP group created can request SNMP messages. |
| **Write View Name** | Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent. |
| **Notify View Name** | Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent. |
| **Security Model** | **SNMPv1** – Specifies that SNMP version 1 will be used.<br>**SNMPv2** – Specifies that SNMP version 2c will be used. The SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) |

| | |
|---|---|
| | and adds some security features.<br>**SNMPv3** – Specifies that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network. |
| **Security Level** | **The Security Level** settings only apply to **SNMPv3.**<br>**NoAuthNoPriv** – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.<br>**AuthNoPriv** – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.<br>**AuthPriv** – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted. |

To implement your new settings, click *Apply*. To return to the **SNMP Group Table**, click the Show All SNMP **Group** Table Entries link.

## SNMP Community Table Configuration

Use this table to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:
An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.
Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.
Read/write or read-only level permission for the MIB objects accessible to the SNMP community.
To configure SNMP Community entries, open the **SNMP V3** folder and click the **SNMP Community Table** link, which will open the following screen:

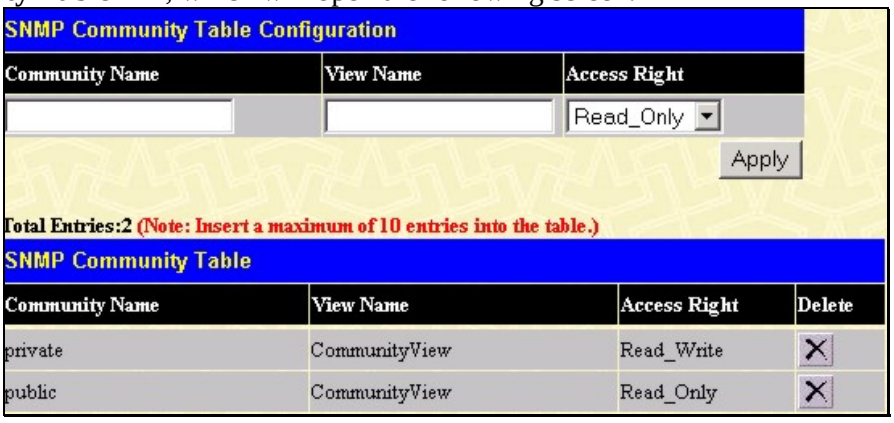



**Figure 7- 27. Community Table Configuration and Table**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **Community Name** | Type an alphanumeric string of up to 33 characters that is used to identify members of an SNMP community. This string is used like a password to give |

| | |
|---|---|
| | remote SNMP managers access to MIB objects in the Switch's SNMP agent. |
| **View Name** | Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table. |
| **Access Right** | **read_only** – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch.<br>**read_write** – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the Switch. |

To implement the new settings, click *Apply*. To delete an entry from the **SNMP Community Table**, click the ✕ under the **Delete** heading, corresponding to the entry you wish to delete.

## SNMP Host Table

Use the **SNMP Host Table** to set up SNMP trap recipients.
Open the **SNMP V3** folder, and click on the **SNMP Host Table** link. This will open the **SNMP Host Table** page, as shown below.
To delete an existing **SNMP Host Table** entry, click the corresponding ✕ under the **Delete** heading.
To display the current settings for an existing **SNMP Group Table** entry, click the blue link for the entry under the **Host IP Address** heading.

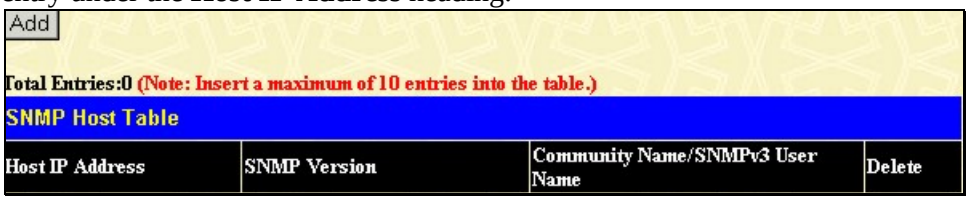



**Figure 7- 28. SNMP Host Table**

To add a new entry to the Switch's **SNMP Group Table**, click the *Add* button in the upper left-hand corner of the **SNMP Host Table** page. This will open the **SNMP Host Table Configuration** page, as shown below.

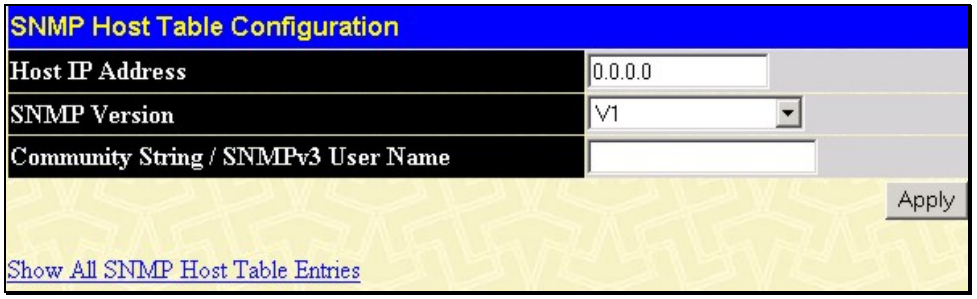



**Figure 7- 29. SNMP Host Table Configuration**

The following parameters can be set:

| Parameter | Description |
|---|---|
| **IP Address** | Type the IP address of the remote management station that will serve as the |

| | |
|---|---|
| | SNMP host for the Switch. |
| **SNMP Version** | **V1** – To specify that SNMP version 1 will be used.<br>**V2** – To specify that SNMP version 2 will be used.<br>**V3-NoAuth-NoPriv** – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.<br>**V3-NoAuth-NoPriv** – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.<br>**V3-Auth-NoPriv** – To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level.<br>**V3-Auth-Priv** – To specify that the SNMP version 3 will be used, with an Auth-Priv security level. |
| **Community String or SNMP V3 User Name** | Type in the community string or SNMP V3 user name as appropriate. |

To implement your new settings, click *Apply*. To return to the **SNMP Host Table**, click the Show All SNMP Host Table Entries link.

## SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the Switch.
To display the Switch's SNMP Engine ID, open the **SNMP V3** folder, and click on the **SNMP Engine ID** link. This will open the **SNMP Engine ID Configuration** window, as shown below.

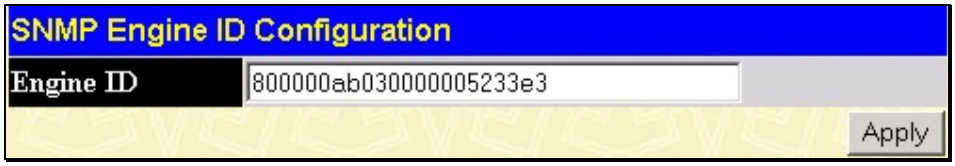



**Figure 7- 30. SNMP Engine ID Configuration**

To change the **Engine ID**, type the new **Engine ID** in the space provided and click the *Apply* button.

# Section 8

# Monitoring

***Port Utilization***
***CPU Utilization***
***Packets***
***Errors***
***Size***
***MAC Address***
***IGMP Snooping Group***
***IGMP Snooping Forwarding***
***VLAN Status***
***Router Port***
***Port Access Control***

## Port Utilization

The **Port Utilization** page displays the percentage of the total available bandwidth being used on the port. Port utilization statistics may be viewed using a line graph or table format.
To view the port utilization, click on the **Monitoring** folder and then the **Port Utilization** link:

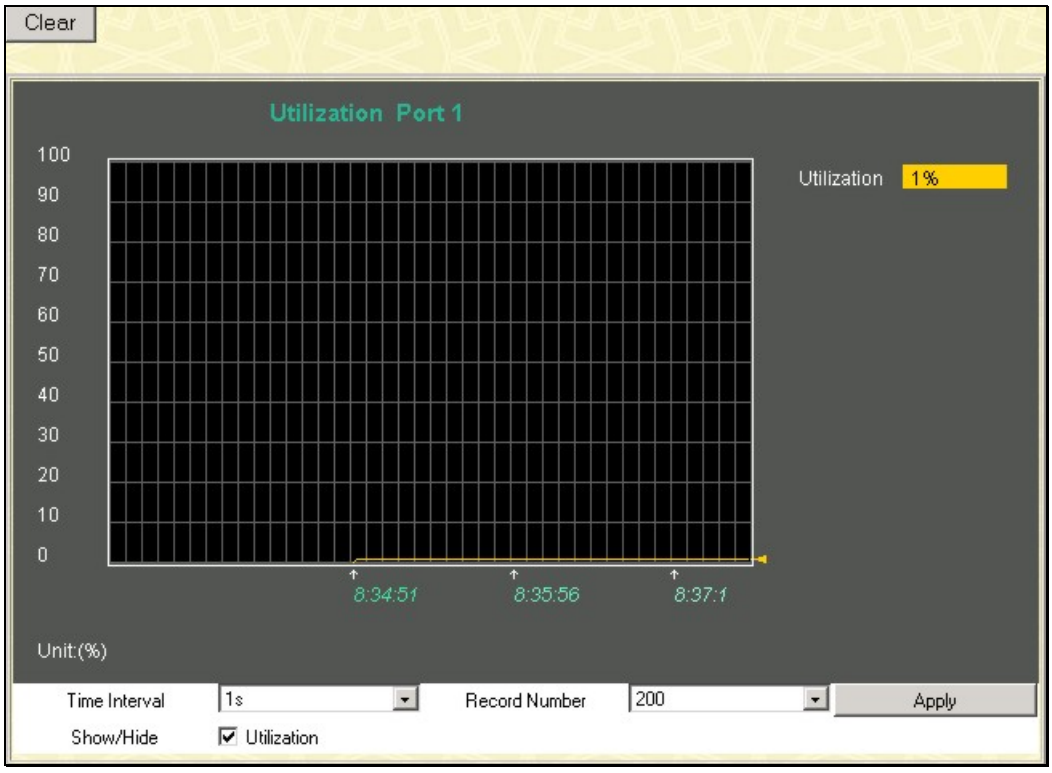



**Figure 8- 1. Port Utilization window**

The following field can be set:

| Parameter | Description |
|---|---|
| **Time Interval** | Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second. |
| **Record Number** | Select number of times the Switch will be polled between *20* and *200*. The default value is *200.* |

Click *Clear* to refresh the graph. Click *Apply* to set changes implemented.

## CPU Utilization

The **CPU Utilization** displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval. To view the **CPU Utilization** window, open the **Monitoring** folder and click the **CPU Utilization** link.

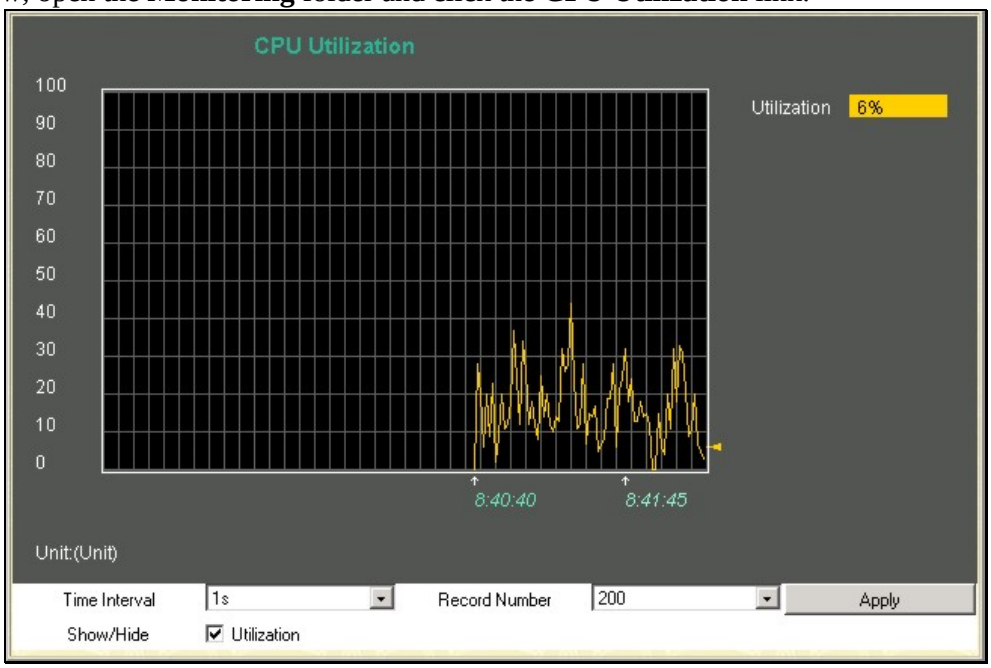



**Figure 8- 2. CPU Utilization graph**

Click *Apply* to implement the configured settings. The window will automatically refresh with new updated statistics
The information is described as follows:

| Parameter | Description |
|---|---|
| **Time Interval [*1s* ]** | Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second. |
| **Record Number [*200*]** | Select number of times the Switch will be polled between *20* and *200*. The default value is *20*. |
| **Utilization** | Check whether or not to display Utilization. |

# Packets

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

## Received(RX)

Click the **Received(RX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of packets received on the Switch.

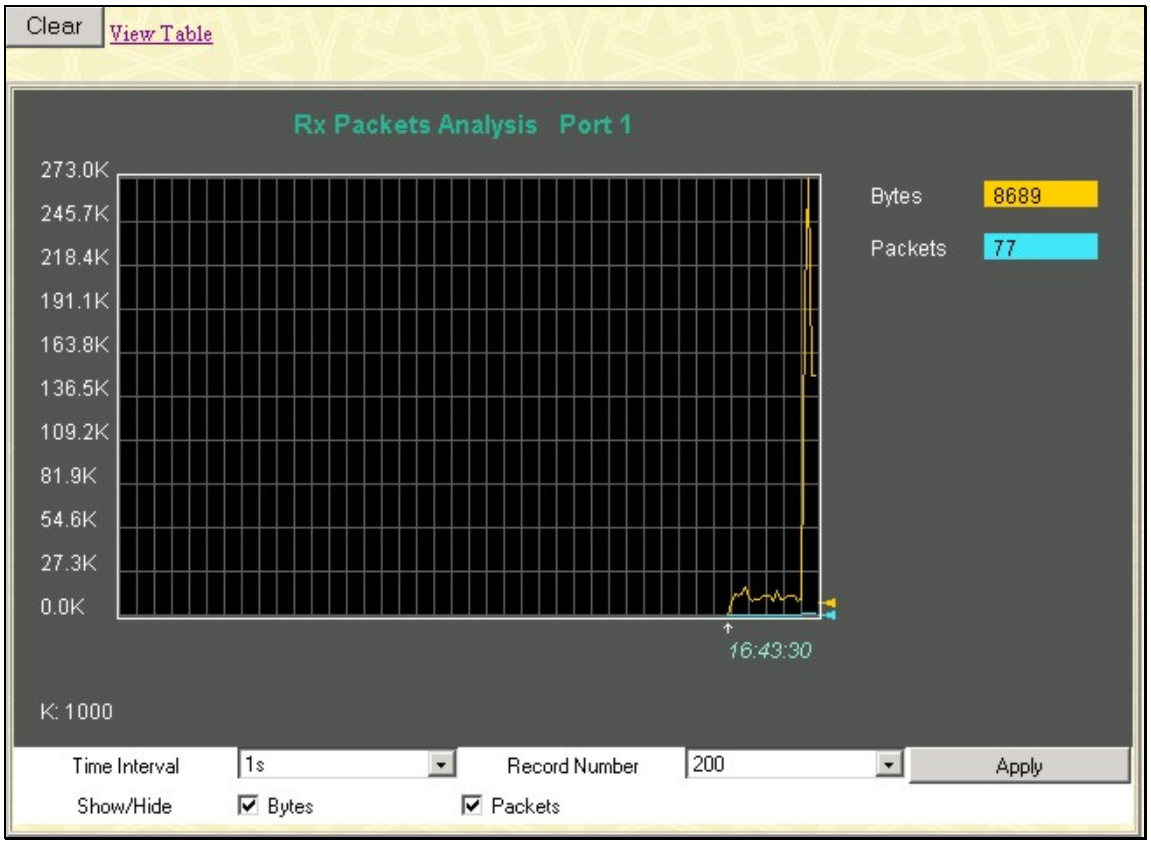



**Figure 8- 3. Rx Packets Analysis window (line graph for Bytes and Packets)**

To view the **Received Packets Table**, click the link **View Table**, which will show the following table:

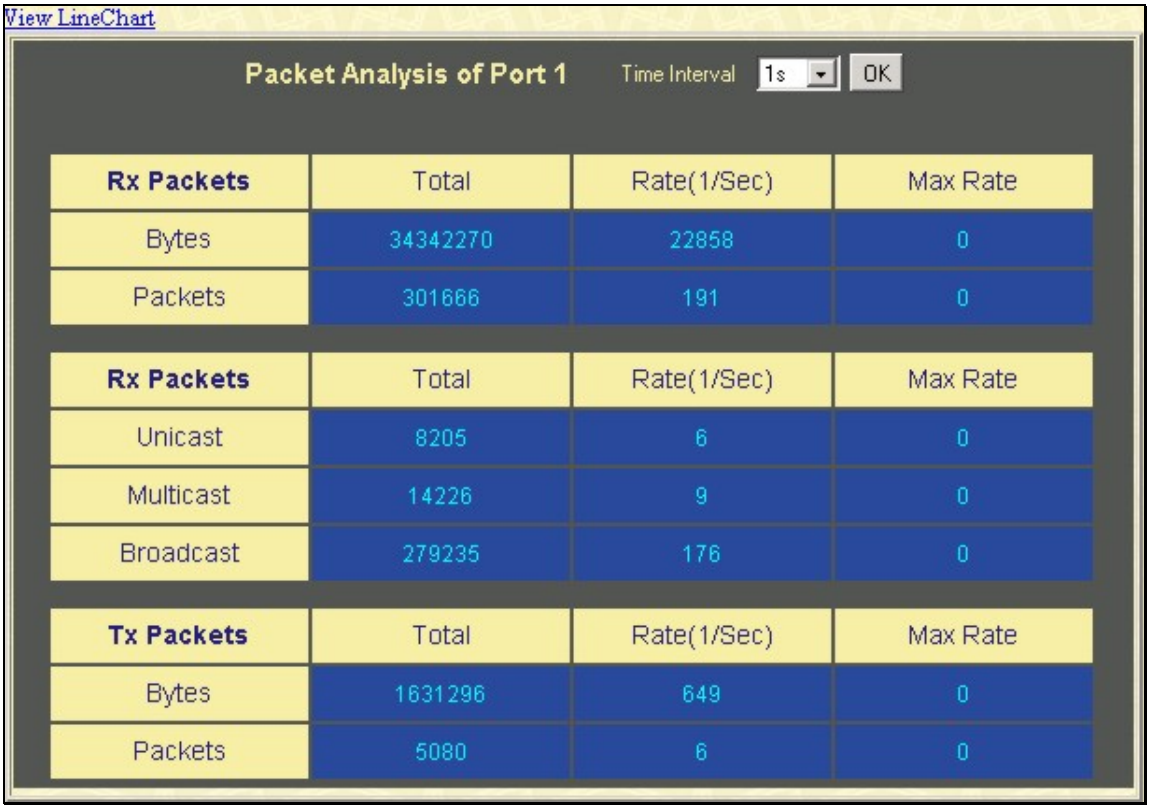



**Figure 8- 4. Rx Packets Analysis window (table for Bytes and Packets)**

The following fields may be set or viewed:

| Parameter | Description |
|---|---|
| **Time Interval [*1s* ]** | Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second. |
| **Record Number [*200*]** | Select number of times the Switch will be polled between *20* and *200*. The default value is *20.* |
| **Bytes** | Counts the number of bytes received on the port. |
| **Packets** | Counts the number of packets received on the port. |
| **Show/Hide** | Check whether to display Bytes and Packets. |
| **Clear** | Clicking this button clears all statistics counters on this window. |
| **View Table** | Clicking this button instructs the Switch to display a table rather than a line graph. |
| **View Line Chart** | Clicking this button instructs the Switch to display a line graph rather than a table. |

## UMB_cast(RX)

Click the **UMB_cast(RX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of UMB cast packets received on the Switch.

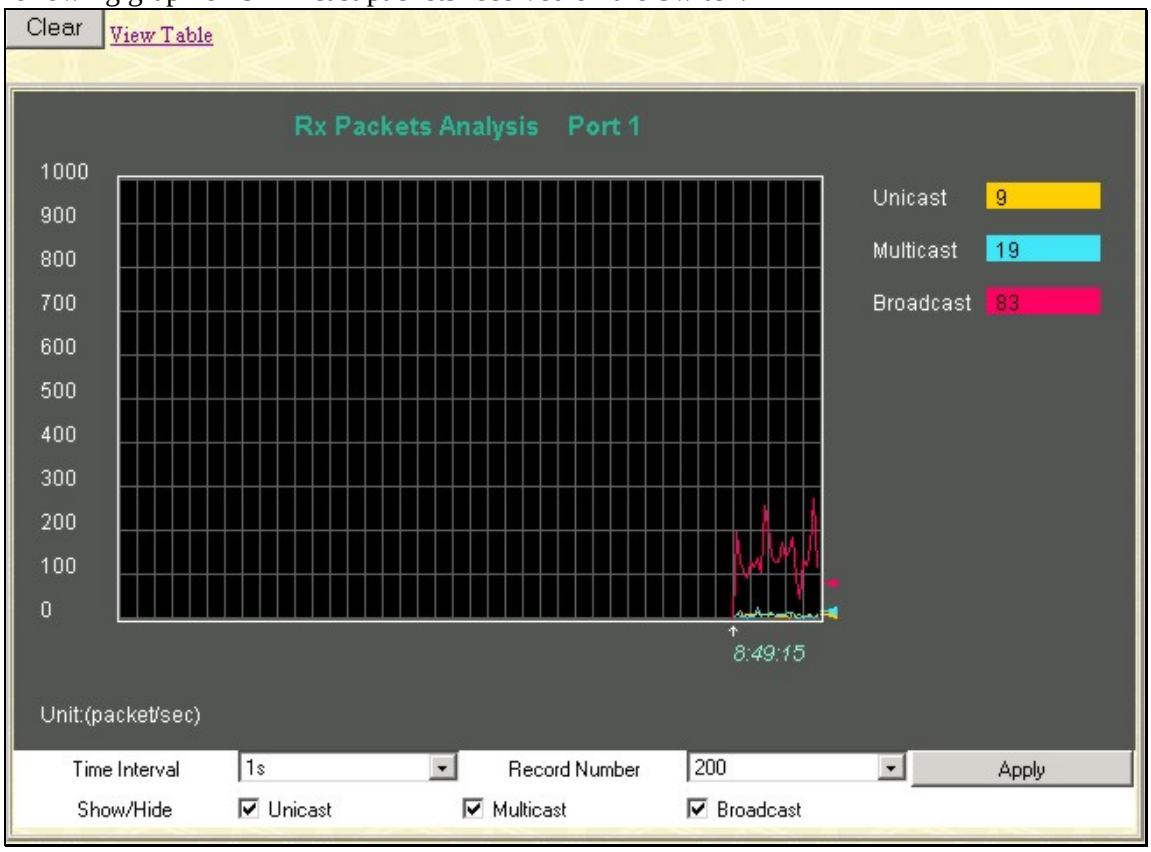



**Figure 8- 5. Rx Packets Analysis window (line graph for Unicast, Multicast, and Broadcast Packets)**

To view the **UMB_cast Table**, click the **View Table** link, which will show the following table:

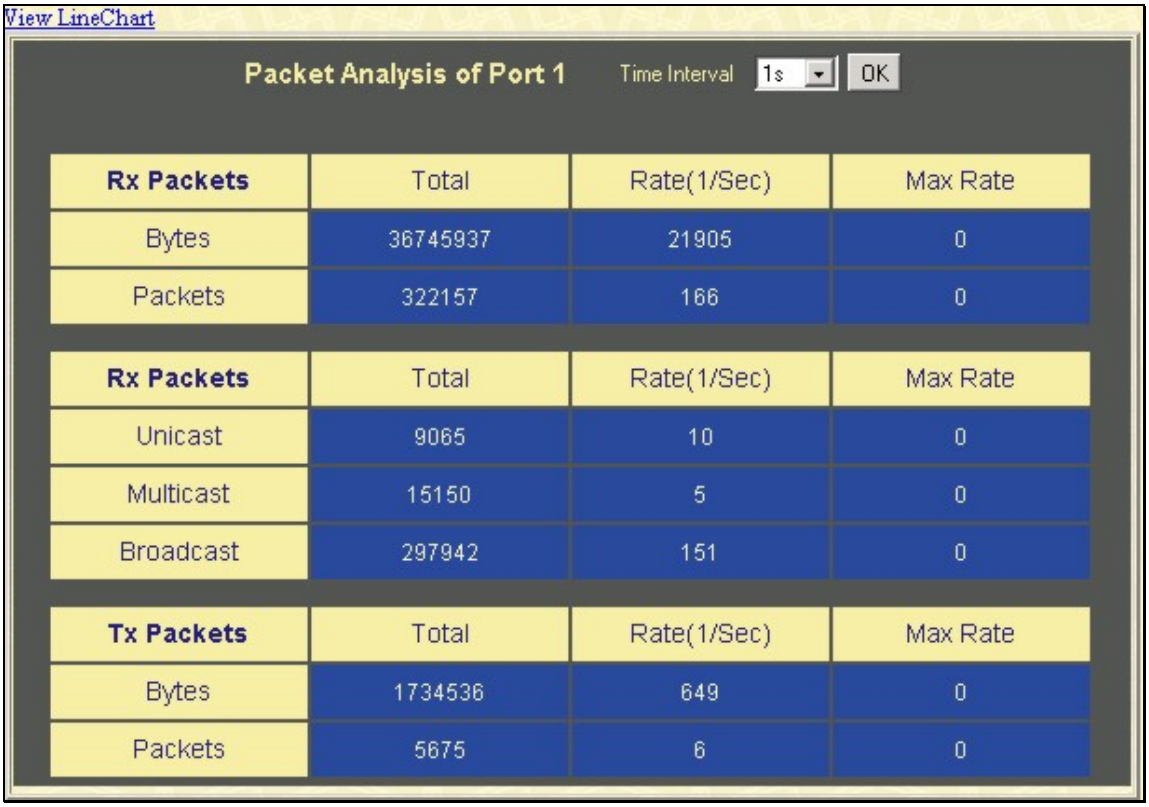



**Figure 6- 64. Rx Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)**

The following fields may be set or viewed:

| Parameter | Description |
|---|---|
| **Time Interval [*1s* ]** | Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second. |
| **Record Number [*200*]** | Select number of times the Switch will be polled between *20* and *200*. The default value is *20.* |
| **Unicast** | Counts the total number of good packets that were received by a unicast address. |
| **Multicast** | Counts the total number of good packets that were received by a multicast address. |
| **Broadcast** | Counts the total number of good packets that were received by a broadcast address. |
| **Show/Hide** | Check whether or not to display Multicast, Broadcast, and Unicast Packets. |
| **Clear** | Clicking this button clears all statistics counters on this window. |
| **View Table** | Clicking this button instructs the Switch to display a table rather than a line graph. |
| **View Line Chart** | Clicking this button instructs the Switch to display a line graph rather than a table. |

## Transmitted (TX)

Click the **Transmitted (TX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of packets transmitted from the Switch.

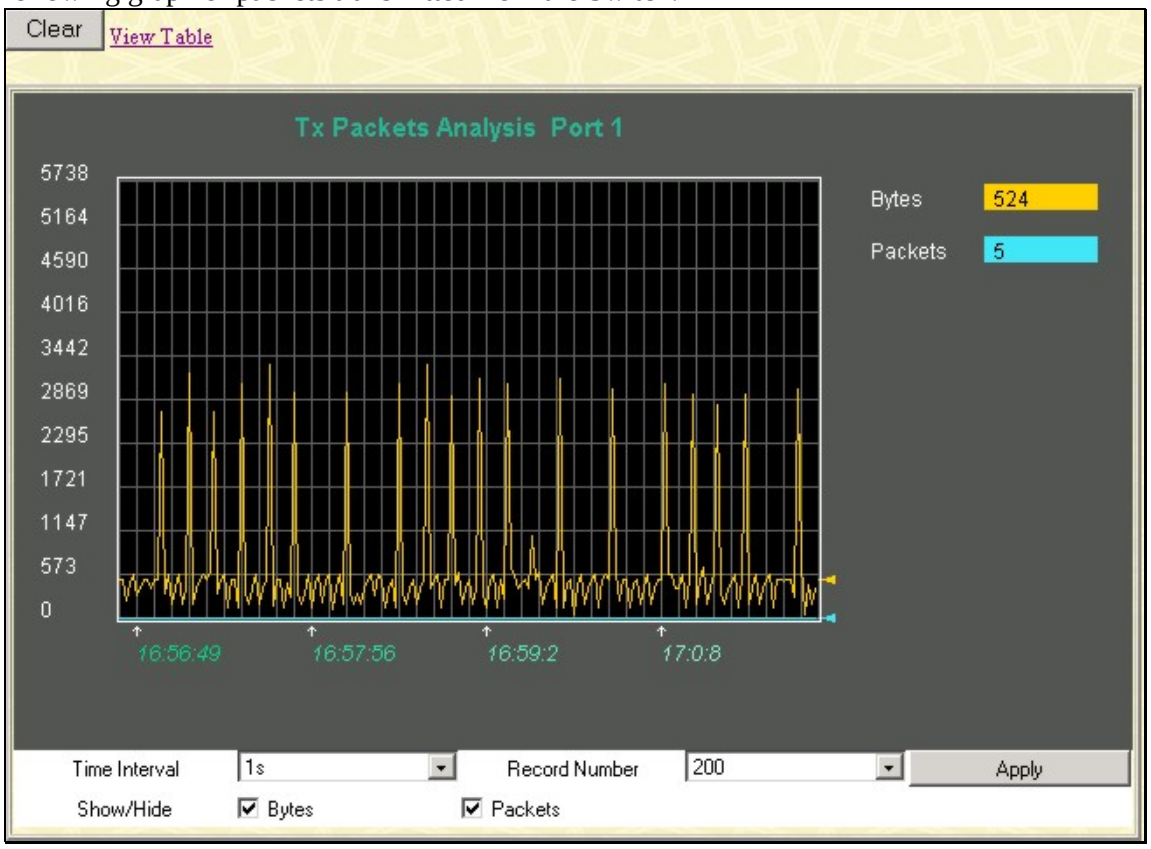



**Figure 8- 6. Tx Packets Analysis window (line graph for Bytes and Packets)**

To view the **UMB_cast Table**, click the link **View Table**, which will show the following table:

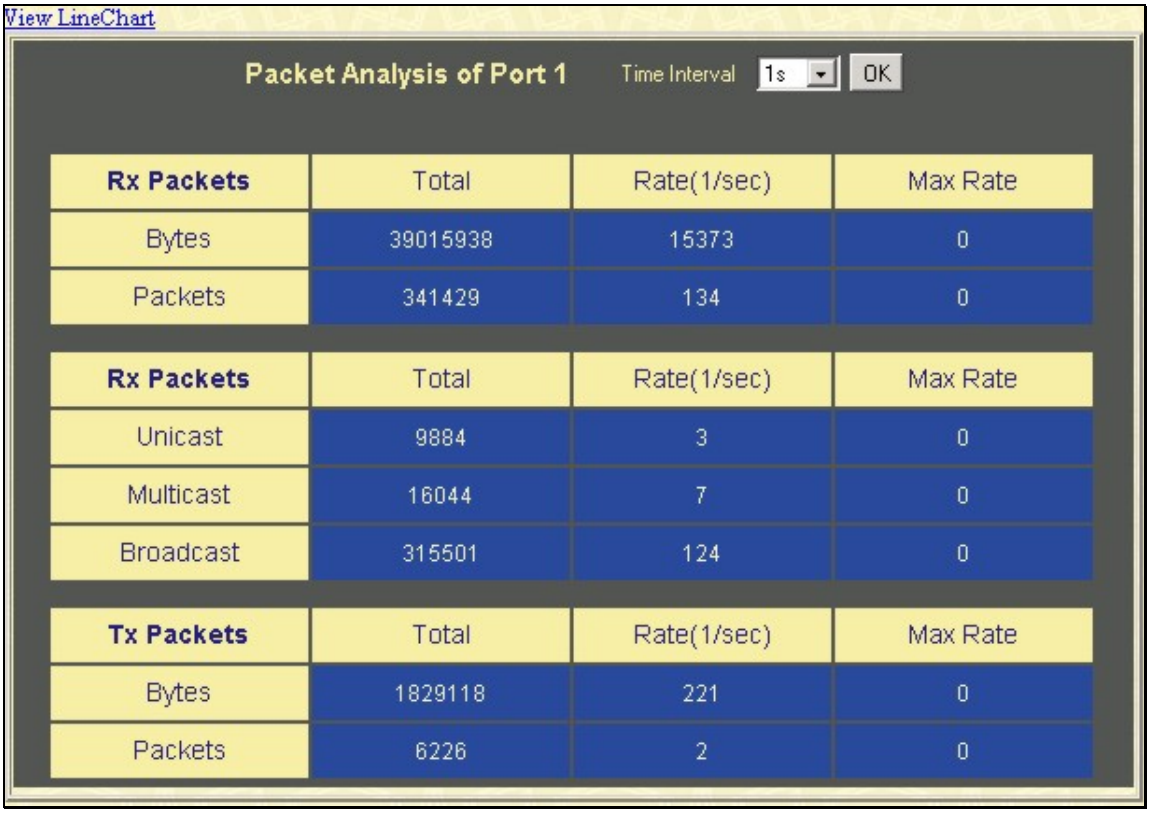



**Figure 8- 7. Tx Packets Analysis window (table for Bytes and Packets)**

The following fields may be set or viewed:

| Parameter | Description |
|---|---|
| **Time Interval [*1s* ]** | Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second. |
| **Record Number [*200*]** | Select number of times the Switch will be polled between *20* and *200*. The default value is *20.* |
| **Bytes** | Counts the number of bytes successfully sent from the port. |
| **Packets** | Counts the number of packets successfully sent on the port. |
| **Show/Hide** | Check whether or not to display Bytes and Packets. |
| **Clear** | Clicking this button clears all statistics counters on this window. |
| **View Table** | Clicking this button instructs the Switch to display a table rather than a line graph. |
| **View Line Chart** | Clicking this button instructs the Switch to display a line graph rather than a table. |

# Errors

The Web Manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

## Received (RX)

Click the **Received (RX)** link in the **Error** folder of the **Monitoring** menu to view the following graph of error packets received on the Switch.

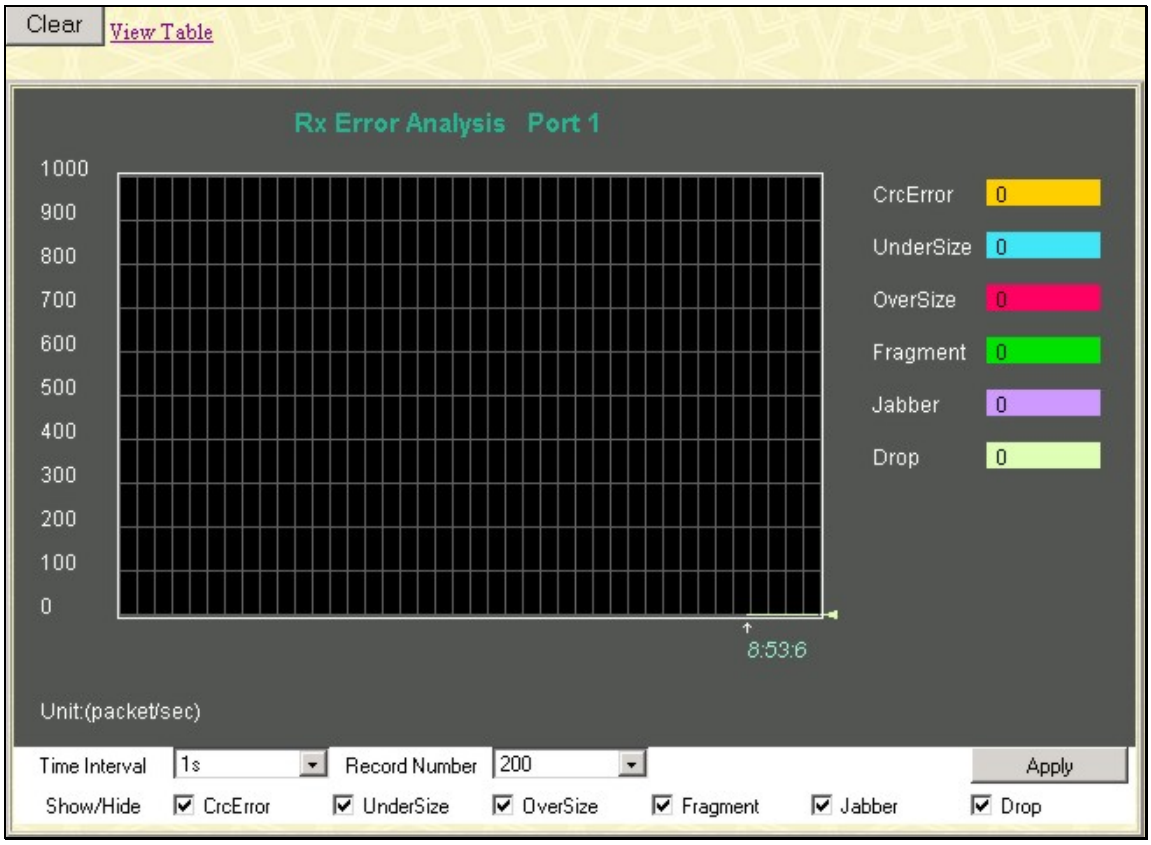



**Figure 8- 8. Rx Error Analysis window (line graph)**

To view the **Received Error Packets Table**, click the link **View Table**, which will show the following table:

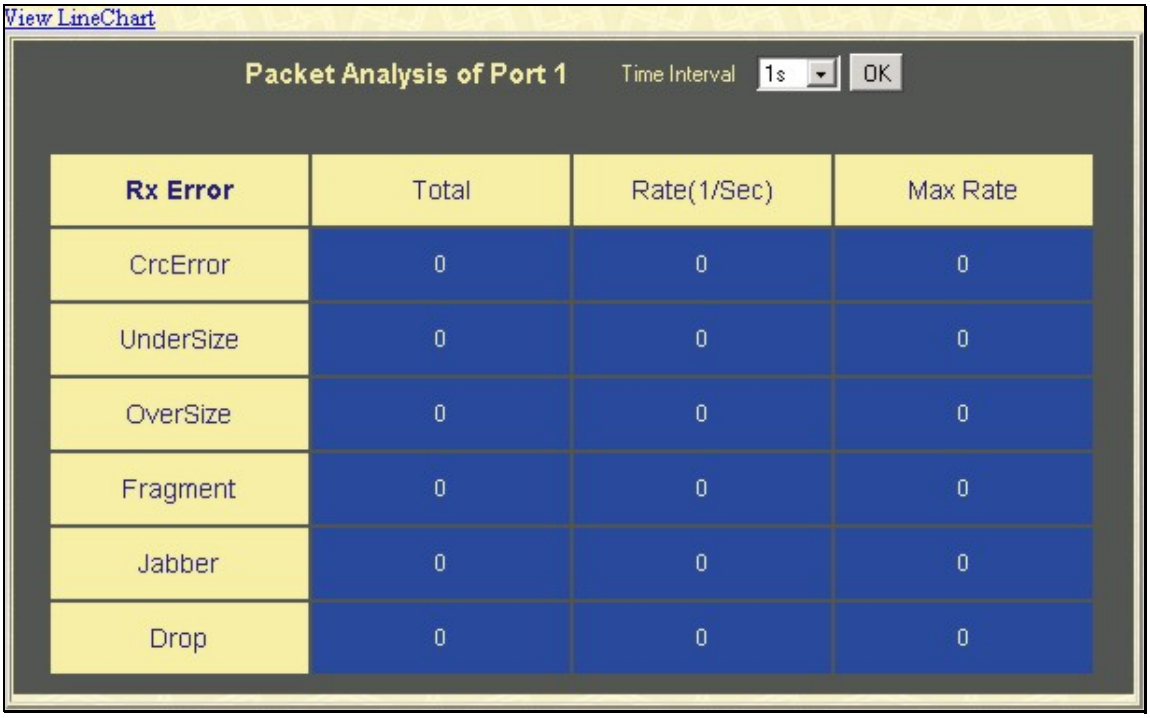



**Figure 8- 9. Rx Error Analysis window (table)**

The following fields can be set:

| Parameter | Description |
|---|---|
| **Time Interval [*1s* ]** | Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second. |
| **Record Number [*200*]** | Select number of times the Switch will be polled between *20* and *200*. The default value is *20.* |
| **CrcError** | Counts otherwise valid packets that did not end on a byte (octet) boundary. |
| **UnderSize** | The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence. |
| **OverSize** | Counts packets received that were longer than 1518 octets, or if a VLAN frame, 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522. |
| **Fragment** | The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions. |
| **Jabber** | The number of packets with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522. |
| **Drop** | The number of packets that are dropped by this port since the last Switch reboot. |
| **Show/Hide** | Check whether or not to display **CrcError**, **UnderSize**, **OverSize**, **Fragment**, **Jabber**, and **Drop** errors. |

| | |
|---|---|
| **Clear** | Clicking this button clears all statistics counters on this window. |
| **View Table** | Clicking this button instructs the Switch to display a table rather than a line graph. |
| **View Line Chart** | Clicking this button instructs the Switch to display a line graph rather than a table. |

## Transmitted (TX)

Click the **Transmitted (TX)** link in the **Error** folder of the **Monitoring** menu to view the following graph of error packets received on the Switch.

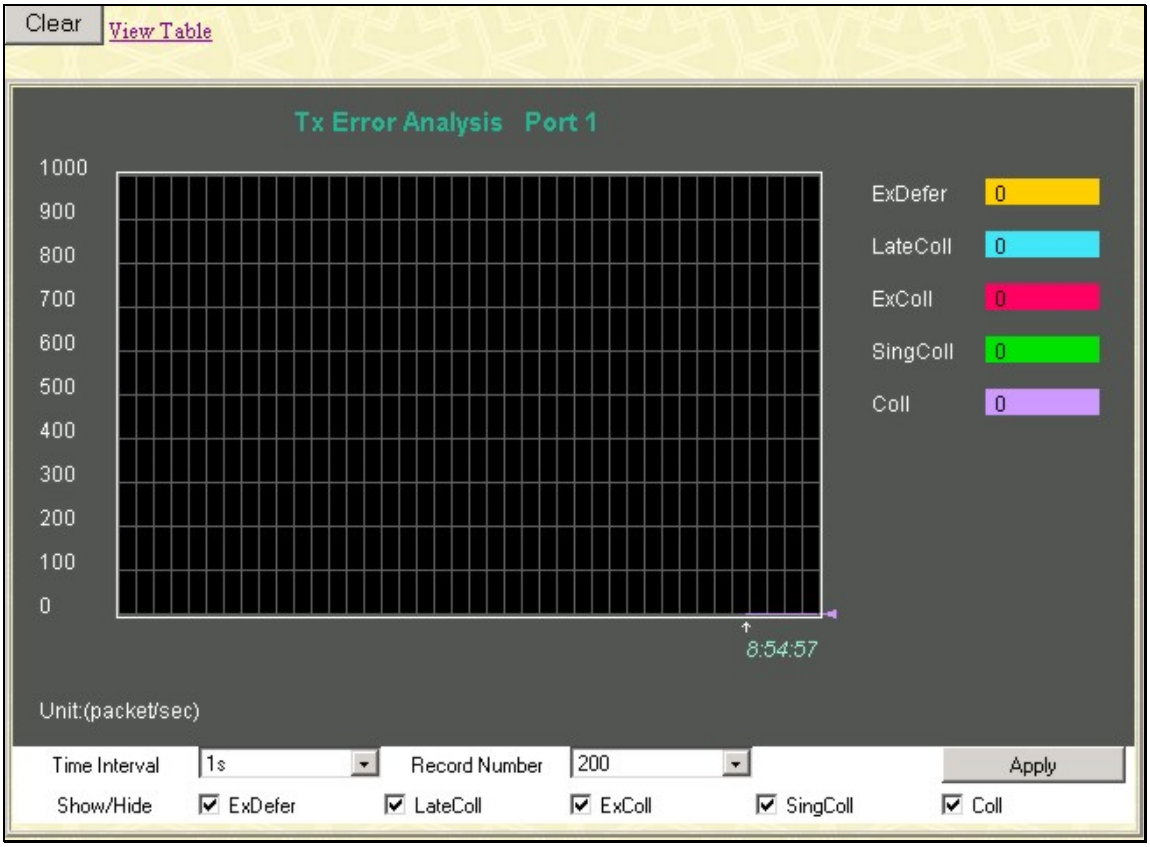



**Figure 8- 10. Tx Error Analysis window (line graph)**

To view the **Transmitted Error Packets Table**, click the link **View Table**, which will show the following table:

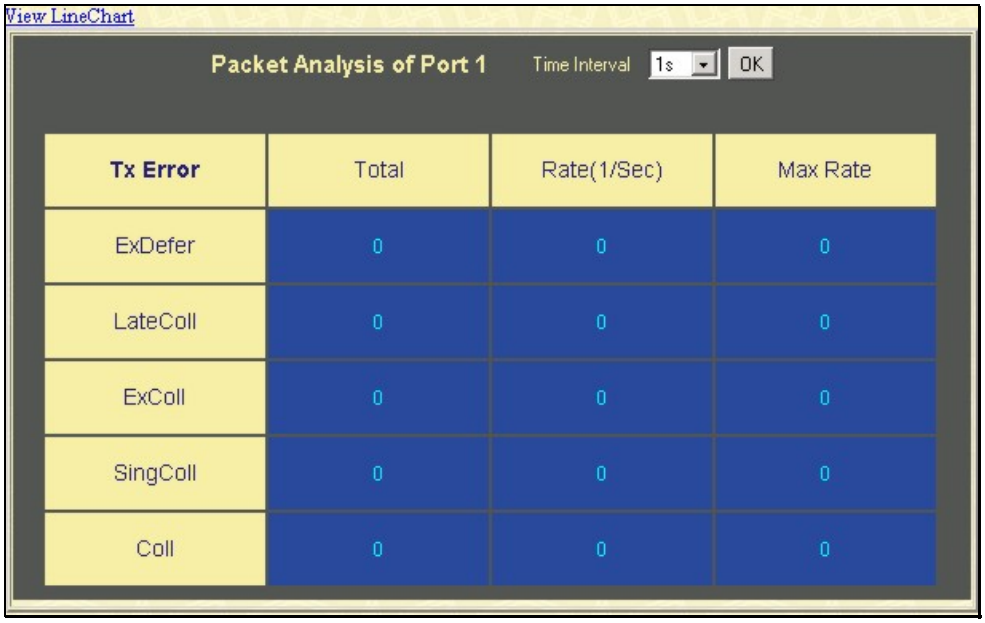



**Figure 8- 11. Tx Error Analysis window (table)**

The following fields may be set or viewed:

| Parameter | Description |
|---|---|
| **Time Interval [*1s* ]** | Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second. |
| **Record Number [*200*]** | Select number of times the Switch will be polled between *20* and *200*. The default value is *20.* |
| **ExDefer** | Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy. |
| **LateColl** | Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet. |
| **ExColl** | Excessive Collisions. The number of packets for which transmission failed due to excessive collisions. |
| **SingColl** | Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision. |
| **Coll** | An estimate of the total number of collisions on this network segment. |
| **Show/Hide** | Check whether or not to display ExDefer, LateColl, ExColl, SingColl, and Coll errors. |
| **Clear** | Clicking this button clears all statistics counters on this window. |
| **View Table** | Clicking this button instructs the Switch to display a table rather than a line graph. |
| **View Line Chart** | Clicking this button instructs the Switch to display a line graph rather than a table. |

## Size

The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered.

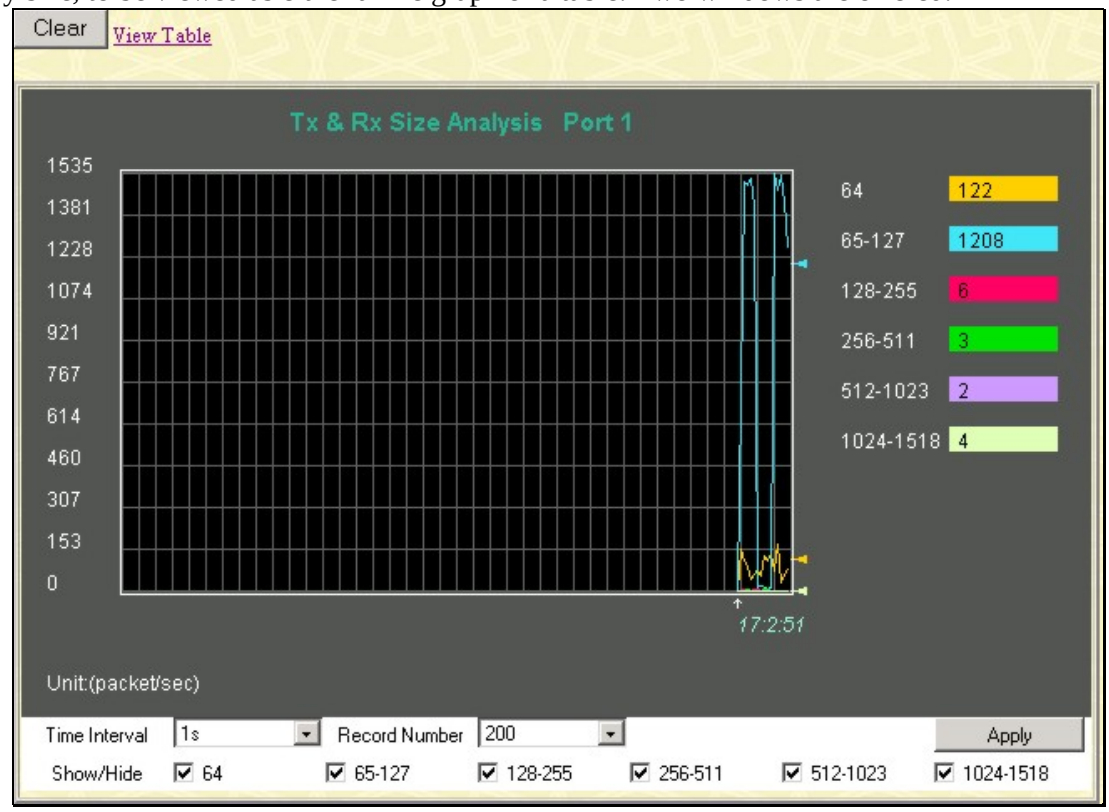
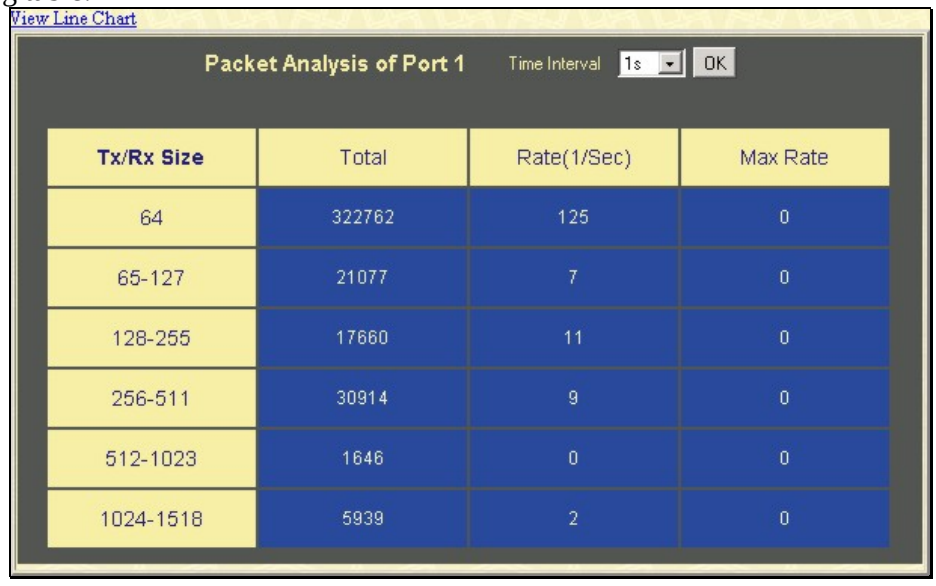



**Figure 8- 12. Rx Size Analysis window (line graph)**

To view the **Packet Size Analysis Table**, click the link **View Table**, which will show the following table:




| Tx/Rx Size | Total | Rate(1/Sec) | Max Rate |
|---|---|---|---|
| 64 | 322762 | 125 | 0 |
| 65-127 | 21077 | 7 | 0 |
| 128-255 | 17660 | 11 | 0 |
| 256-511 | 30914 | 9 | 0 |
| 512-1023 | 1646 | 0 | 0 |
| 1024-1518 | 5939 | 2 | 0 |

**Figure 8- 13. Rx Size Analysis window (table)**

The following fields can be set or viewed:

| Parameter | Description |
|---|---|
| **Time Interval [*1s* ]** | Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second. |
| **Record Number [*200*]** | Select number of times the Switch will be polled between *20* and *200*. The default value is *20.* |
| **64** | The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). |
| **65-127** | The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). |
| **128-255** | The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). |
| **256-511** | The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). |
| **512-1023** | The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). |
| **1024-1518** | The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). |
| **Show/Hide** | Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received. |
| **Clear** | Clicking this button clears all statistics counters on this window. |
| **View Table** | Clicking this button instructs the Switch to display a table rather than a line graph. |
| **View Line Chart** | Clicking this button instructs the Switch to display a line graph rather than a table. |

# MAC Address

This allows the Switch's dynamic MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.
To view the **MAC Address** forwarding table, from the **Monitoring** menu, click the **MAC Address** link:

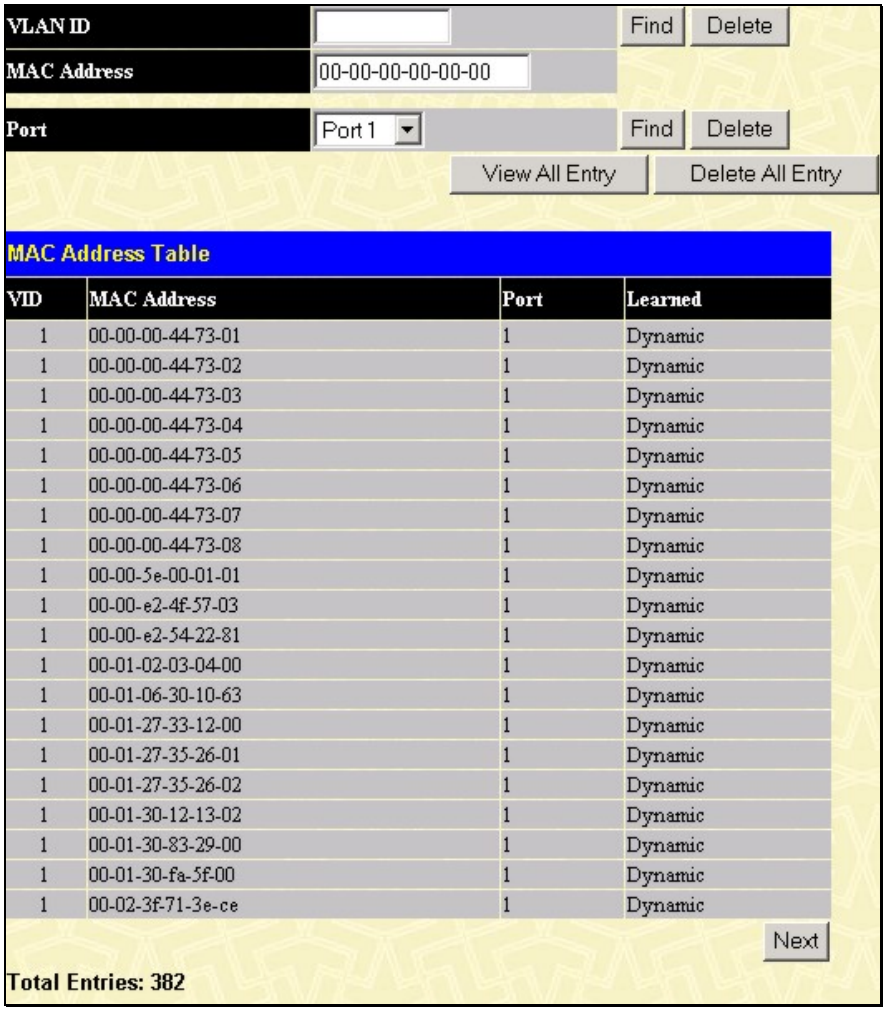



**Figure 8- 14. MAC Address Table**

The following fields can be viewed or set:

| Parameter | Description |
|---|---|
| **VLAN ID** | Enter a VLAN ID for the forwarding table to be browsed by. |
| **MAC Address** | Enter a MAC address for the forwarding table to be browsed by. |
| **Find** | Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address. |
| **VID** | The VLAN ID of the VLAN the port is a member of. |
| **MAC Address** | The MAC address entered into the address table. |
| **Port** | The port that the MAC address above corresponds to. |
| **Learned** | How the switch discovered the MAC address. The possible entries are *Dynamic*, *Self*, and *Static*. |
| **Next** | Click this button to view the next page of the address table. |

# IGMP Snooping Group

IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch. The number of IGMP reports that were snooped is displayed in the **Reports** field.
To view the **IGMP Snooping** table, click **IGMP Snooping Group** on the **Monitoring** menu:

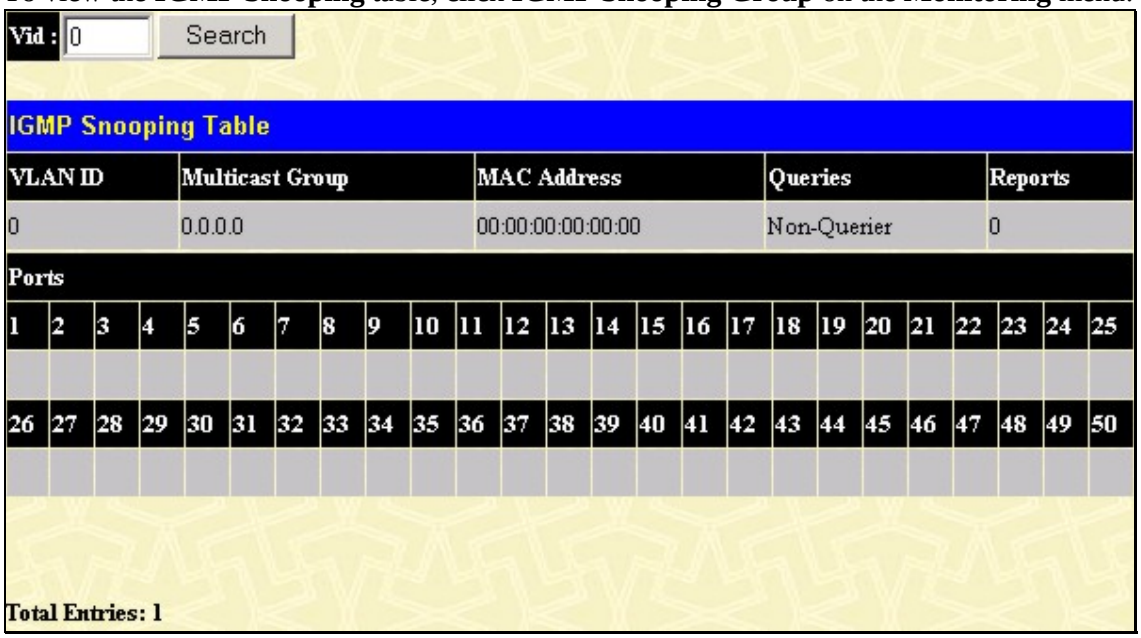



**Figure 8- 15. IGMP Snooping Table**

The user may search the **IGMP Snooping Table** by VLAN ID (VID) by entering the VID in the top left hand corner and clicking *Search*.

The following field can be viewed:

| Parameter | Description |
|---|---|
| **VLAN ID** | The VLAN ID (VID) of the multicast group. |
| **Multicast Group** | The IP address of the multicast group. |
| **MAC Address** | The MAC address of the multicast group. |
| **Queries** | A read only field showing the status of the Querier State. Disabled implies that the Switch is not transmitting IGMP Snooping Query packets, while Enabled means those packets are being transmitted. |
| **Reports** | The total number of reports received for this group. |
| **Port Map** | These are the ports where the IGMP packets were snooped are displayed. |

**Note**: To configure IGMP snooping for the DES-3350, go to the **Configuration** folder and select **IGMP**. Configuration and other information concerning IGMP snooping may be found in Section 6 of this manual under **Configuring IGMP**.

## IGMP Snooping Forwarding

This window will display the current IGMP snooping forwarding table entries currently configured on the Switch. To view the following screen, open the **Monitoring** folder and click the **IGMP Snooping Forwarding** link.

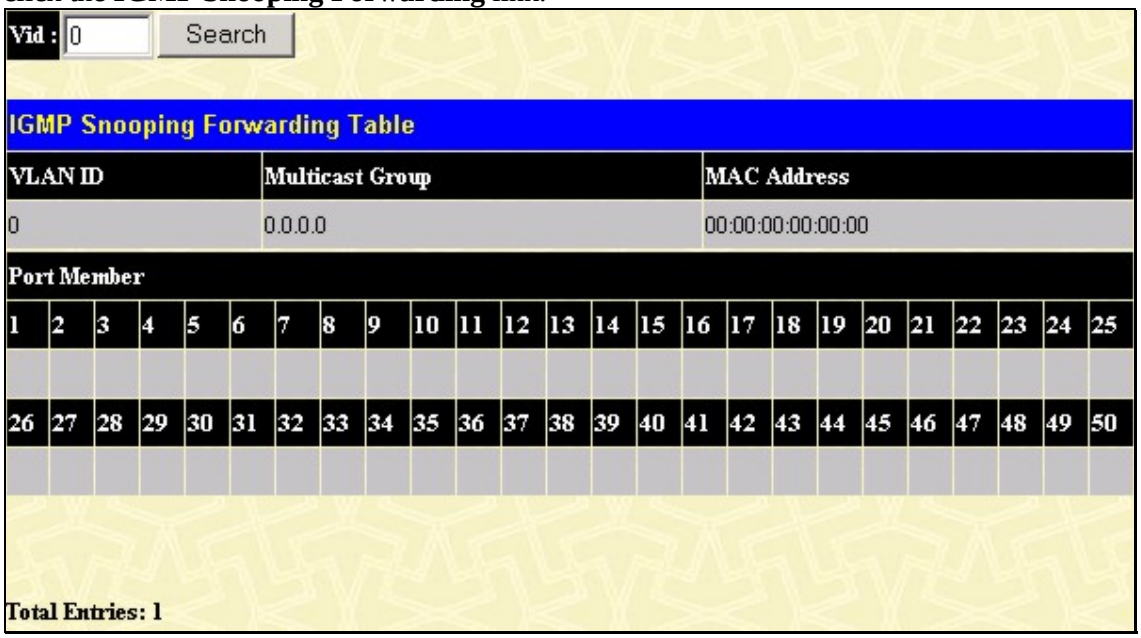



**Figure 8- 16. IGMP Snooping Forwarding Table**

The user may search the **IGMP Snooping Table** by VID using the top left hand corner *Search.*
The following field can be viewed:

| Parameter | Description |
|---|---|
| **VLAN ID** | The VLAN ID (VID) of the multicast group. |
| **Multicast Group** | The IP address of the multicast group. |
| **MAC Address** | The MAC address of the multicast group. |
| **Port Map** | These are the ports where the IGMP packets were snooped are displayed. |

## VLAN Status

This allows the VLAN status for each of the Switch's ports to be viewed by the VLAN. This window displays the ports on the Switch that are currently Egress or Untagged ports. To view the following table, open the Monitoring folder and click the VLAN Status Link.

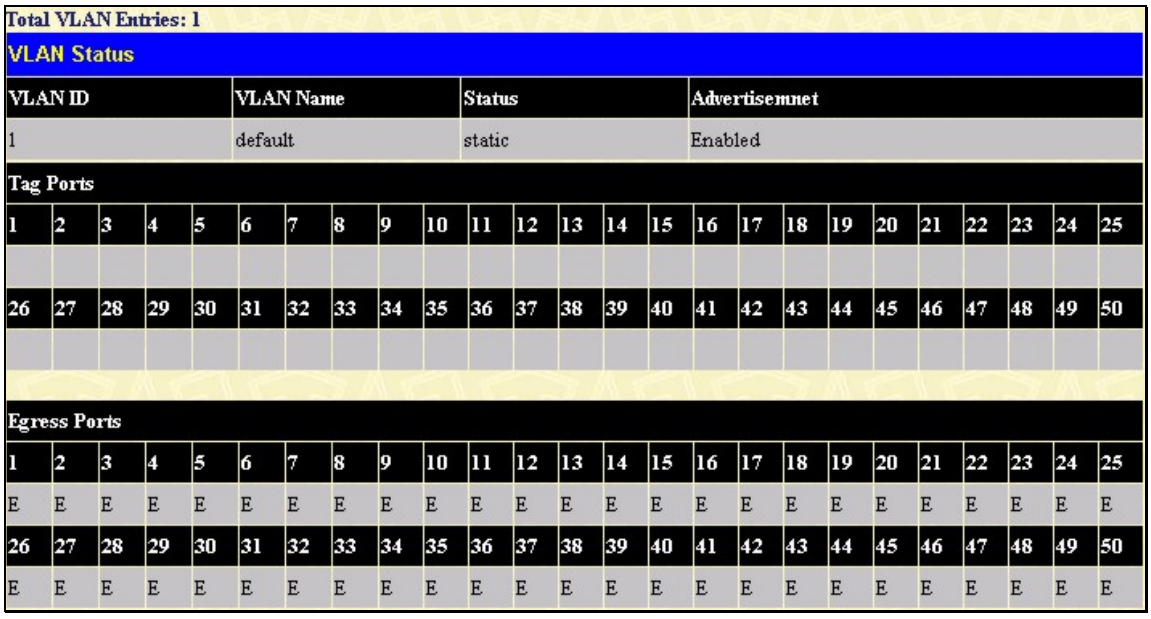



**Figure 8- 17. VLAN Status window**

## Browse Router Port

This displays which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by **S**. A router port that is dynamically configured by the Switch is designated by **D**. To view the following window, open the Monitoring folder and click the Router port link.

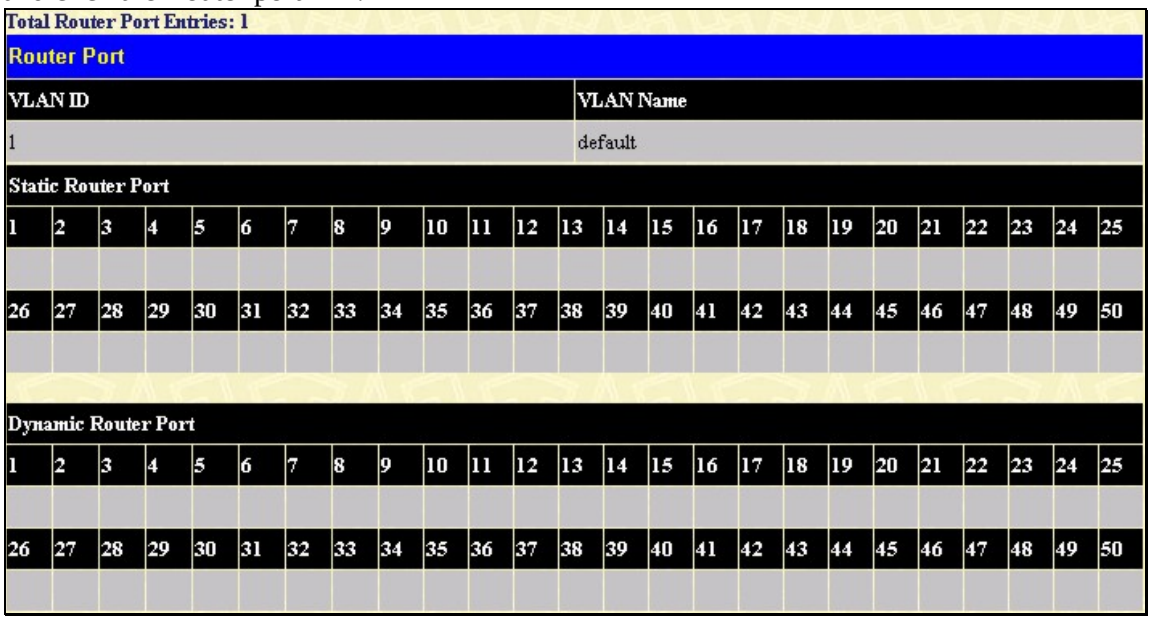



**Figure 8- 18. Router Port window.**

# Port Access Control

The following section describes the 802.1X Status on the Switch. To view the Authenticator state, click **Monitoring > Port Access Control > Authenticator State.**

## Authenticator State

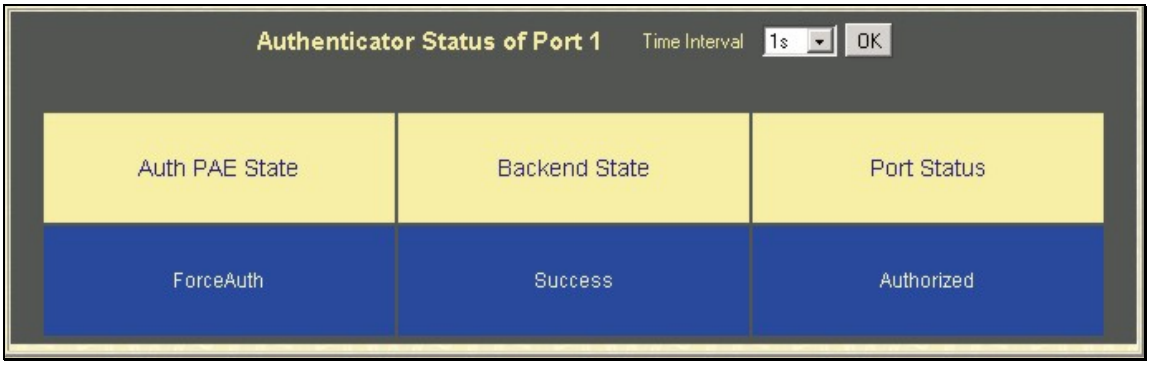



**Figure 8- 19. Authenticator Status window**

This window displays the **Authenticator Status** for an individual port. To select a port, click a port on the front panel display. A polling interval between *1* and *60* seconds can be set using the drop-down menu at the top of the window and clicking *OK*.
The information on this window is described as follows:

| Parameter | Description |
|---|---|
| **Auth PAE State** | The Authenticator PAE state value can be: *Initialize*, *Disconnected*, *Connecting*, *Authenticating*, *Authenticated*, *Aborting*, *Held*, *Force_Auth*, *Force_Unauth*, or *N/A*. *N/A* (Not Available) indicates that the port's authenticator capability is disabled. |
| **Backend State** | The Backend Authentication state can be *Request*, *Response*, *Success*, *Fail*, *Timeout*, *Idle*, *Initialize*, or *N/A*. *N/A* indicates that the port's authenticator capability is disabled. |
| **PortStatus** | Auth Controlled Port Status can be *Authorized*, *Unauthorized*, or *N/A*. |

# Section 9

# Maintenance

***TFTP Services***
***Switch History***
***Ping Test***
***Save Changes***
***Reboot Services***
***Logout***

## TFTP Services

Trivial File Transfer Protocol (TFTP) services allow the Switch's firmware to be upgraded by transferring a new firmware file from a TFTP server to the Switch. A configuration file can also be loaded into the Switch from a TFTP server. Switch settings can be saved to the TFTP server, and a history log can be uploaded from the Switch to the TFTP server.

### Download Firmware From TFTP Server

To update the Switch's firmware, open the **TFTP Services** folder in the **Maintenance** folder and click the **Download Firmware from TFTP** link:

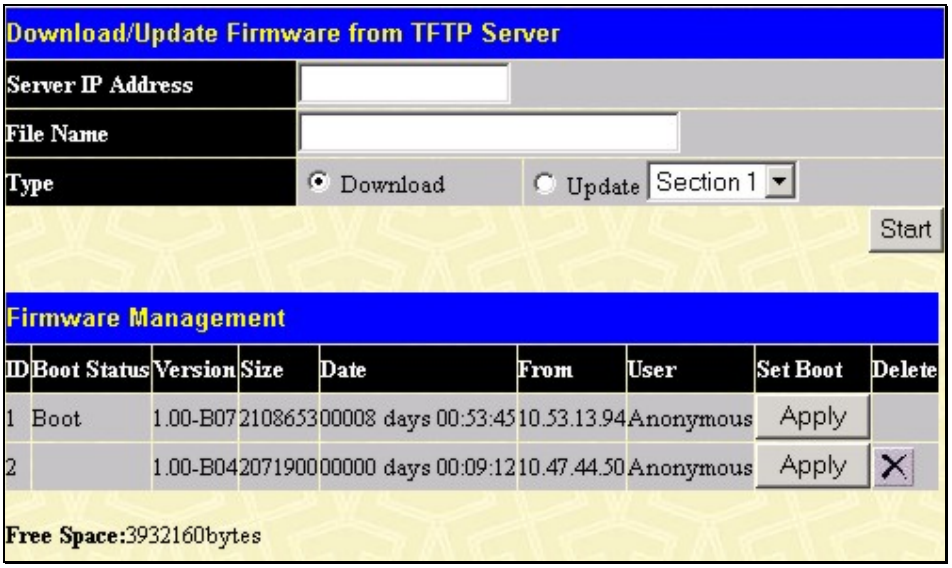



**Figure 9- 1. Download/Update Firmware from TFTP Server**

The Switch can hold two firmware versions for the user, which can be specified in the Type field by clicking the **Update** radio button and selecting the **Section ID** (*Section 1* or *Section 2*). To download or update firmware, configure the following fields and click *Start*.

| Parameter | Description |
|---|---|
| **Server IP** | Enter the IP address of the server from which you wish to download firmware. |
| **File Name** | Specify the path and filename of the firmware on the Server. |

| | |
|---|---|
| **Type** | Specify the purpose of the firmware:<br>*Download*: Clicking this radio button will specify a download to the Switch. This will be the firmware that the Switch will immediately use.<br>*Update***:** Clicking this radio button will save the firmware to the Switch's memory but not configure the Switch for this firmware. The Switch may hold two firmware versions specified as Section 1 and Section 2. |

Information about firmware on the Switch can be viewed in the **Firmware Management** table in the same screen. It holds the following information:

| Parameter | Description |
|---|---|
| **ID** | The user defined Section ID of the firmware on the Switch. |
| **Boot Status** | The firmware that is currently being run on the Switch will be identified in this field with the term "Boot." |
| **Version** | The runtime version of the firmware. |
| **Size** | The size, in bytes, of the firmware. |
| **Date** | The date that the firmware was added to the Switch. |
| **From** | The IP address of the Server from which the firmware came. |
| **User** | The name of the user who downloaded the firmware. |
| **Set Boot** | Click the Apply button in this field to set the firmware version to be used upon the next boot up of the Switch. |
| **Delete** | Click the in this column to permanently delete the corresponding firmware from the Switch |

## Download Settings from TFTP Server

To download a settings file from a TFTP server, click on the **TFTP Service** folder in the **Maintenance** folder and then click the **Download Settings from TFTP Server** link:

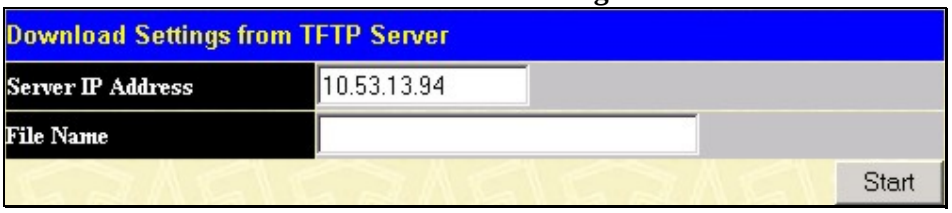



**Figure 9- 2. Download Configuration**

Enter the IP address of the TFTP server and specify the location of the switch settings file on the TFTP server.
Click *Start* to record the IP address of the TFTP server and to initiate the file transfer.

## Upload Settings to TFTP Server

To upload the switch settings to a TFTP server, click on the **TFTP Service** folder in the **Maintenance** folder and then click the **Upload Settings to TFTP Server** link:

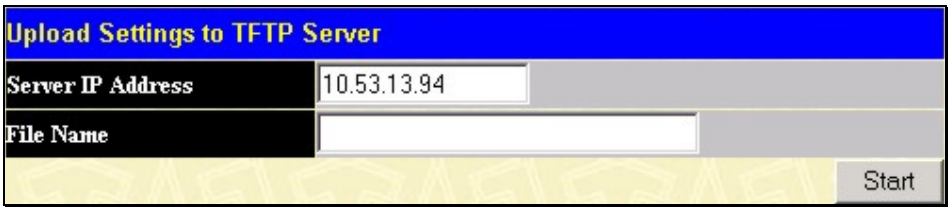



**Figure 9- 3. Upload Settings to TFTP Server window**

Enter the IP address of the TFTP server and the path and filename for the switch settings on the TFTP server.
Click *Start* to record the IP address of the TFTP server and to initiate the file transfer.

## Upload Log to TFTP Server

To upload the switch history log file to a TFTP server, open the **TFTP Service** folder in the **Maintenance** folder and then click the **Upload log to TFTP Server** link:

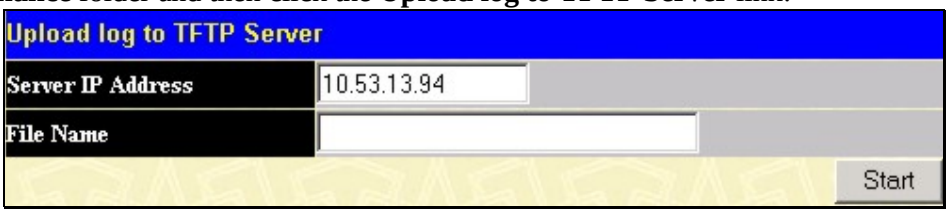
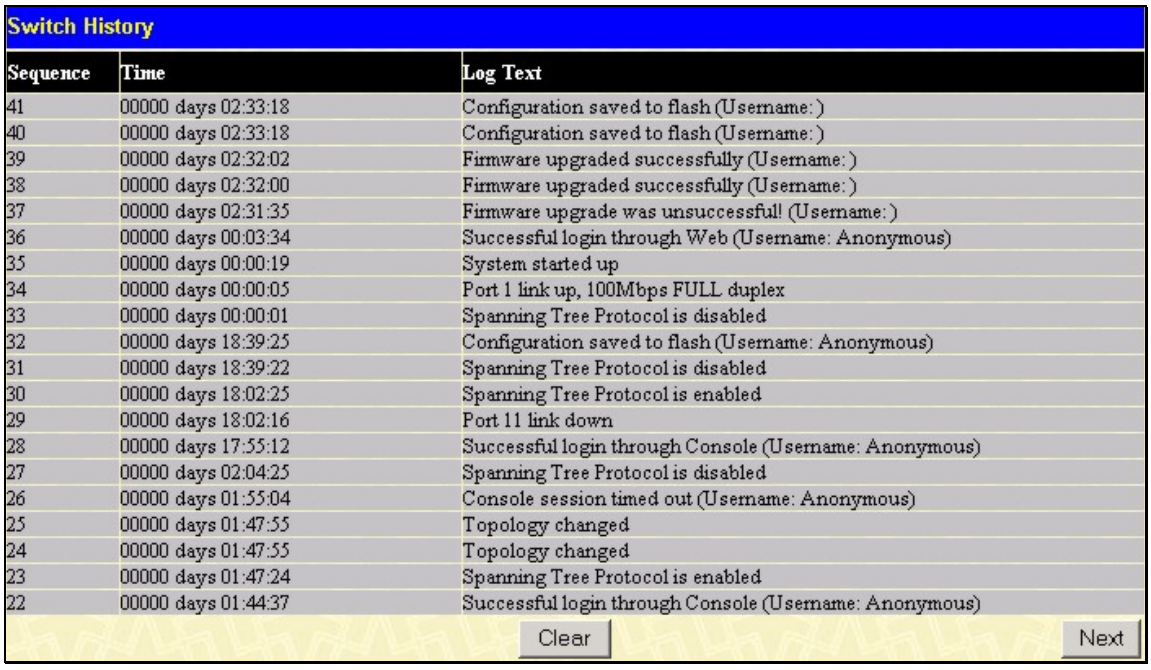



**Figure 9- 4. Upload Log to TFTP Server window**

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server.
Click *Start* to record the IP address of the TFTP server and to initiate the file transfer.

## Switch History

The Web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed. To view the Switch history log, open the **Maintenance** folder and click the **Switch History** link.



Switch History

| Sequence | Time | Log Text |
|---|---|---|
| 41 | 00000 days 02:33:18 | Configuration saved to flash (Username: ) |
| 40 | 00000 days 02:33:18 | Configuration saved to flash (Username: ) |
| 39 | 00000 days 02:32:02 | Firmware upgraded successfully (Username: ) |
| 38 | 00000 days 02:32:00 | Firmware upgraded successfully (Username: ) |
| 37 | 00000 days 02:31:35 | Firmware upgrade was unsuccessful! (Username: ) |
| 36 | 00000 days 00:03:34 | Successful login through Web (Username: Anonymous) |
| 35 | 00000 days 00:00:19 | System started up |
| 34 | 00000 days 00:00:05 | Port 1 link up, 100Mbps FULL duplex |
| 33 | 00000 days 00:00:01 | Spanning Tree Protocol is disabled |
| 32 | 00000 days 18:39:25 | Configuration saved to flash (Username: Anonymous) |
| 31 | 00000 days 18:39:22 | Spanning Tree Protocol is disabled |
| 30 | 00000 days 18:02:25 | Spanning Tree Protocol is enabled |
| 29 | 00000 days 18:02:16 | Port 11 link down |
| 28 | 00000 days 17:55:12 | Successful login through Console (Username: Anonymous) |
| 27 | 00000 days 02:04:25 | Spanning Tree Protocol is disabled |
| 26 | 00000 days 01:55:04 | Console session timed out (Username: Anonymous) |
| 25 | 00000 days 01:47:55 | Topology changed |
| 24 | 00000 days 01:47:55 | Topology changed |
| 23 | 00000 days 01:47:24 | Spanning Tree Protocol is enabled |
| 22 | 00000 days 01:44:37 | Successful login through Console (Username: Anonymous) |

Clear Next

**Figure 9- 5. Switch History window**

The Switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager. Clicking **Next** at the bottom of the window will allow you to display all the switch Trap Logs.
The information is described as follows:

| Parameter | Description |
|---|---|
| **Sequence** | A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first. |
| **Time** | Displays the time in days, hours, and minutes since the Switch was last restarted. |
| **Log Text** | Displays text describing the event that triggered the history log entry. |

Click *Clear* to clear the **Switch History** log. Click *Next* to go to the next page of the **Switch History Log**.

# Ping Test

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or echoes the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

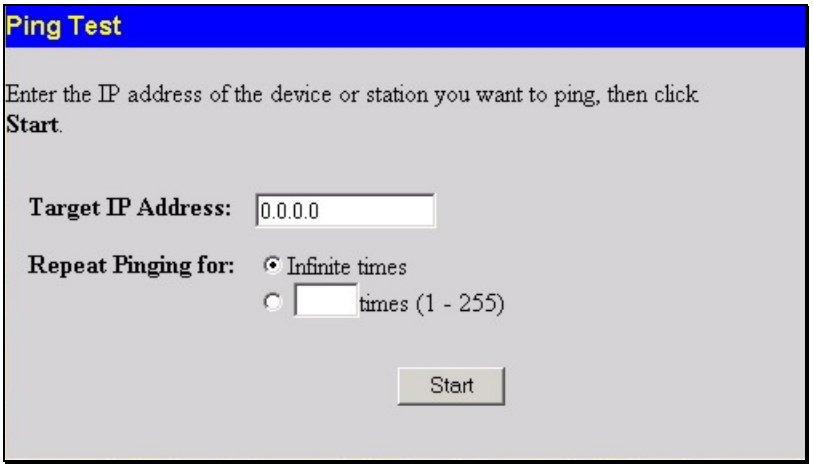

Ping Test
Enter the IP address of the device or station you want to ping, then click Start.
Target IP Address:
0.0.0.0
Repeat Pinging for:
Infinite times
times (1 - 255)
Start

**Figure 9- 6. Ping Test**

The user may use **Infinite times** checkbox, in the **Repeat Pinging for:** field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the *Target IP Address* by clicking its radio button and entering a number between 1 and 255. Click *Start* to initiate the Ping program.

## Saving Changes

The DES-3550 has two levels of memory, normal RAM and non-volatile or NV-RAM. Configuration changes are made effective by clicking the *Apply* button. When this is done, the settings will be immediately applied to the switching software in RAM and will immediately take effect.

Some settings, though, require you to restart the Switch before they will take effect. Restarting the Switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the Switch.

To retain any configuration changes permanently, click the **Save Changes** link in the **Maintenance** folder. The following screen will appear:

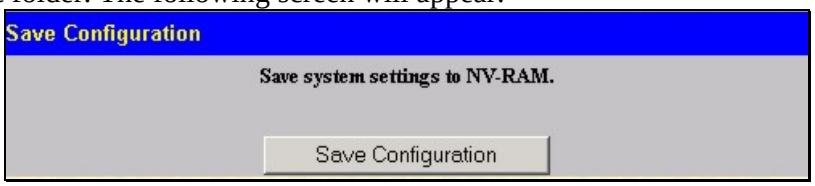



**Figure 9- 7. Save Changes Screen**

Click the **Save Configuration** button to save the current switch configuration in NV-RAM. The following dialog box will confirm that the configuration has been saved:

**Figure 9- 8. Save Configuration Confirmation**

Click the **OK** button to continue.

Once the switch configuration settings have been saved to NV-RAM, they become the default settings for the Switch. These settings will be used every time the Switch is rebooted.

# Reboot Services

The following section will aid the user in rebooting and resetting the Switch using the following windows, described in detailed.

## Reboot Device

The following window is used to restart the Switch.
All of the configuration information, entered from the last time **Save Changes** was executed, will be lost. Click the **Reboot** button to restart the Switch.

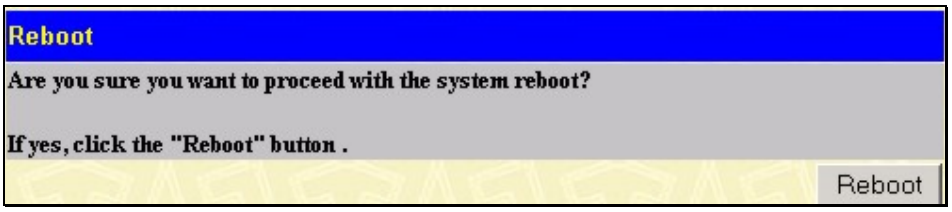



**Figure 9- 9. Reboot window**

# Reset

The **Reset** function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

**NOTE:** Only the **Reset System** option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. **Reset System** will return the Switch's configuration to the state it was when it left the factory.

**Reset** gives the option of retaining the Switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the Switch is reset with this option enabled, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.

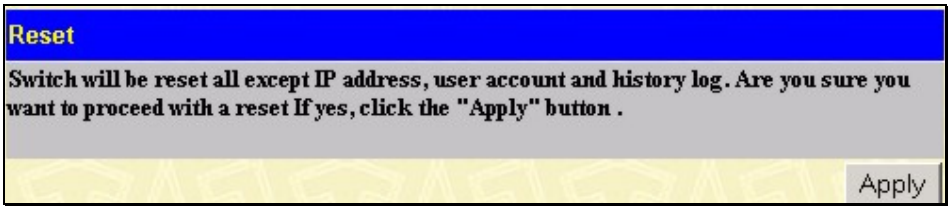

Reset
Switch will be reset all except IP address, user account and history log. Are you sure you want to proceed with a reset If yes, click the "Apply" button .
Apply

**Figure 9- 10. Reset window**

In addition, the **Reset System** option is added to reset all configuration parameters to their factory defaults, save these parameters to the Switch's non-volatile RAM, and then restart the Switch. This option is equivalent to **Reset Config** (above) followed by **Save Changes**.

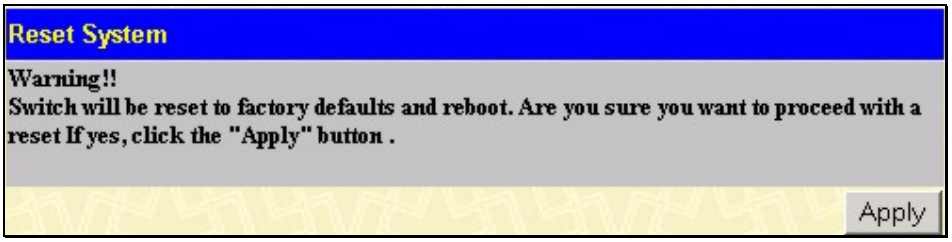

Reset System
Warning!!
Switch will be reset to factory defaults and reboot. Are you sure you want to proceed with a reset If yes, click the "Apply" button .
Apply

**Figure 9- 11. Reset System window**

The **Reset Config** option will reset all of the Switch's configuration parameters to their factory defaults, without saving these default values to the Switch's non-volatile RAM. If the Switch is reset with this option enabled, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.

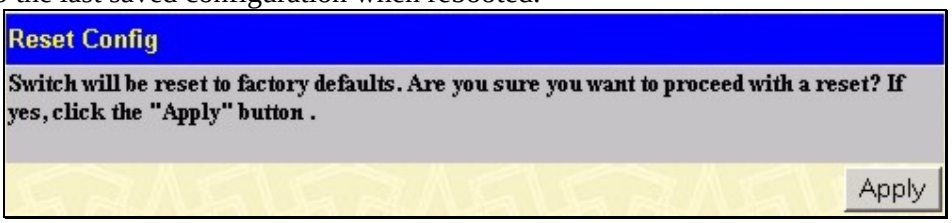

Reset Config
Switch will be reset to factory defaults. Are you sure you want to proceed with a reset? If yes, click the "Apply" button .
Apply

**Figure 9- 12. Reset Config window**

## Logout

Use the **Logout** page to logout of the Switch's Web-based management agent by clicking on the **Log Out** button.

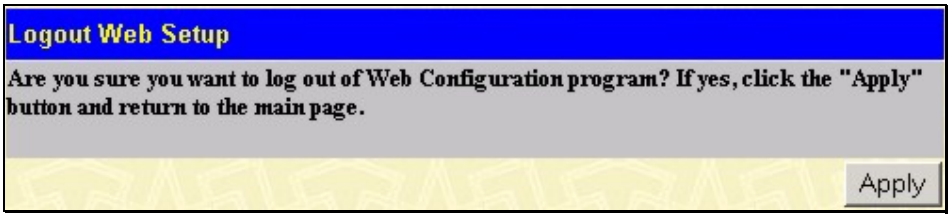

Logout Web Setup
Are you sure you want to log out of Web Configuration program? If yes, click the "Apply" button and return to the main page.
Apply

**Figure 9- 13. Logout window**

**Section 10**

# Single IP Management

***Single IP Management (SIM) Overview***
***Topology***
***Firmware Upgrade***
***Configuration Backup/Restore***

## Single IP Management (SIM) Overview

Simply put, Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. There are some advantages in implementing the "**Single IP Management**" feature:

1. SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
2. SIM can reduce the number of IP address needed in your network.
3. SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

Switches using **Single IP Management** (labeled here as **SIM**) must conform to the following rules:

→ SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface. SIM grouping has no effect on the normal operation of the Switch in the user's network.

→ There are three classifications for switches using SIM. The **Commander Switch (CS)**, which is the master switch of the group, **Member Switch (MS)**, which is a switch that is recognized by the CS as a member of a SIM group, and a **Candidate Switch (CaS)**, which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.

→ A SIM group can only have one Commander Switch (CS).

→ All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.

→ A SIM group accepts up to 32 switches (numbered 0-31), including the Commander Switch (numbered 0).

→ There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.

→ If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.

→ SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that is more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The DES-3550 may take on three different roles:

→ **Commander Switch (CS)** – This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:

It has an IP Address.
It is not a command switch or member switch of another Single IP group.
It is connected to the member switches through its management VLAN.

→ **Member Switch (MS)** – This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:

It is not a CS or MS of another IP group.

It is connected to the CS through the CS management VLAN.

→ **Candidate Switch (CaS)** – This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group through an automatic function of the DES-3550, or by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:

It is not a CS or MS of another Single IP group.

It is connected to the CS through the CS management VLAN

The following rules also apply to the above roles:

→ Each device begins in a Commander state.

→ CS's must change their role to CaS and then to MS, to become a MS of a SIM group. Thus, the CS cannot directly be converted to a MS.

→ The user can manually configure a CS to become a CaS.

A MS can become a CaS by:

→ Being configured as a CaS through the CS.

→ If report packets from the CS to the MS time out.

→ The user can manually configure a CaS to become a CS.

→ The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional DES-3550 switches may join the group either by an automatic method or by manually configuring the switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, and then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CS becomes a MS, it automatically becomes a member of the first SNMP community (include read/write and read only) to which the CS belongs. However, if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

## SIM Using the Web Interface

All DES-3550 switches are set as **Candidate (CaS)** switches, as their factory default configuration and the Single IP Management feature will be disabled. To enable SIM for the Switch using the Web interface, go to the **Single IP Management** folder and click the **SIM Settings** link, revealing the following window.

**Figure 10- 1. SIM Settings window (*disabled*)**

Change the **SIM State** to *Enabled* using the pull down menu and click *Apply*. The screen will then refresh and the SIM Settings window will look like this:

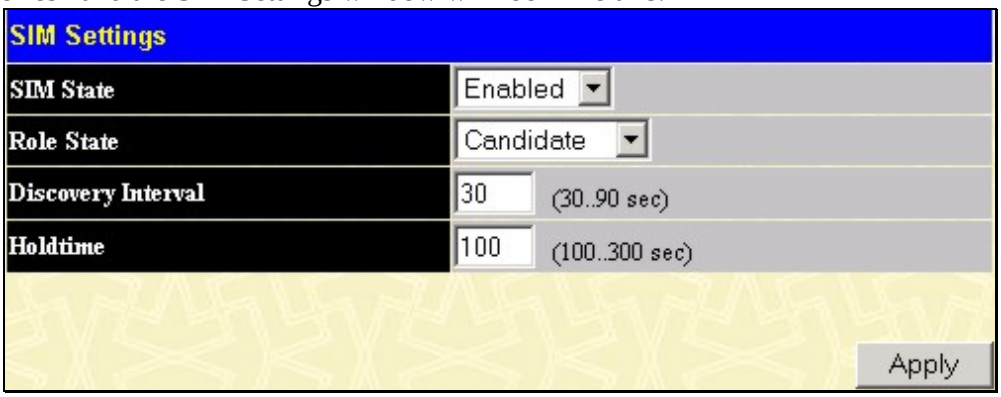



**Figure 10- 2. SIM Settings window (*enabled*)**

The following parameters can be set:

| Parameters | Description |
|---|---|
| **SIM State** | Use the pull down menu to either enable or disable the SIM state on the Switch. *Disabled* will render all SIM functions on the Switch inoperable. |
| **Role State** | Use the pull down menu to change the SIM role of the Switch. The two choices are:<br>*Candidate* – A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role of the DES-3550.<br>*Commander* – Choosing this parameter will make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM. |
| **Discovery Interval** | The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to a Commander Switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the *Discovery Interval* from 30 to 90 seconds. |
| **Holdtime** | This parameter may be set for the time, in seconds that the Switch will hold information sent to it from other switches, utilizing the *Discovery Interval*. The user may set the hold time from 100 to 300 seconds. |

Click *Apply* to implement the settings changed.

After enabling the Switch to be a **Commander Switch (CS)**, the **Single IP Management** folder will then contain three added links to aid the user in configuring SIM through the web, including **Topology**, **Firmware Upgrade**, and **Configuration Backup/Restore**.

## Topology

The Topology window will be used to configure and manage the Switch within the SIM group and requires Java script to function properly on your computer. The following message should appear the first time the user clicks the **Topology** link in the **Single IP Management** folder.

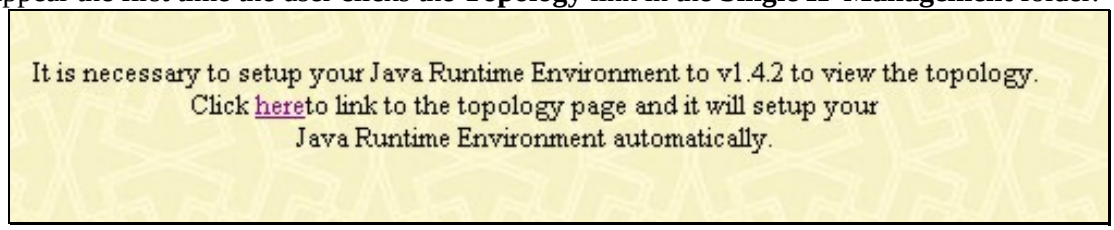

It is necessary to setup your Java Runtime Environment to v1.4.2 to view the topology.
Click hereto link to the topology page and it will setup your
Java Runtime Environment automatically.

**Figure 10- 3. Java window**

Clicking the here link will setup the Java Runtime Environment on your server and lead you to the topology window, as seen below.

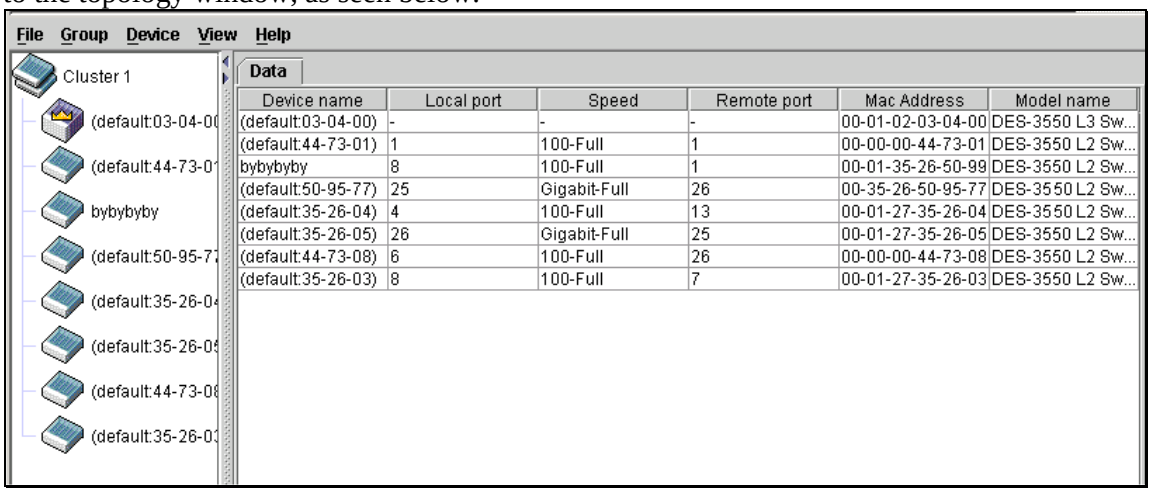

File Group Device View Help
Cluster 1
(default:03-04-0
(default:44-73-0
bybybyby
(default:50-95-7
(default:35-26-0
(default:35-26-0
(default:44-73-0
(default:35-26-0
Data
Device name | Local port | Speed | Remote port | Mac Address | Model name
(default:03-04-00) | - | - | - | 00-01-02-03-04-00 | DES-3550 L3 Sw...
(default:44-73-01) | 1 | 100-Full | 1 | 00-00-00-44-73-01 | DES-3550 L2 Sw...
bybybyby | 8 | 100-Full | 1 | 00-01-35-26-50-99 | DES-3550 L2 Sw...
(default:50-95-77) | 25 | Gigabit-Full | 26 | 00-35-26-50-95-77 | DES-3550 L2 Sw...
(default:35-26-04) | 4 | 100-Full | 13 | 00-01-27-35-26-04 | DES-3550 L2 Sw...
(default:35-26-05) | 26 | Gigabit-Full | 25 | 00-01-27-35-26-05 | DES-3550 L2 Sw...
(default:44-73-08) | 6 | 100-Full | 26 | 00-00-00-44-73-08 | DES-3550 L2 Sw...
(default:35-26-03) | 8 | 100-Full | 7 | 00-01-27-35-26-03 | DES-3550 L2 Sw...

**Figure 10- 4. Single IP Management window-Tree View**

The Tree View window holds the following information under the Data tab:

| Parameter | Description |
|---|---|
| **Device Name** | This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it. |
| **Local Port** | Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field. |
| **Speed** | Displays the connection speed between the CS and the MS or CaS. |
| **Remote Port** | Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field. |
| **MAC Address** | Displays the MAC Address of the corresponding Switch. |
| **Model Name** | Displays the full Model Name of the corresponding Switch. |

To view the **Topology Map**, click the **View** menu in the toolbar and then **Topology**, which will produce the following screen. The **Topology View** will refresh itself periodically (20 seconds by default).

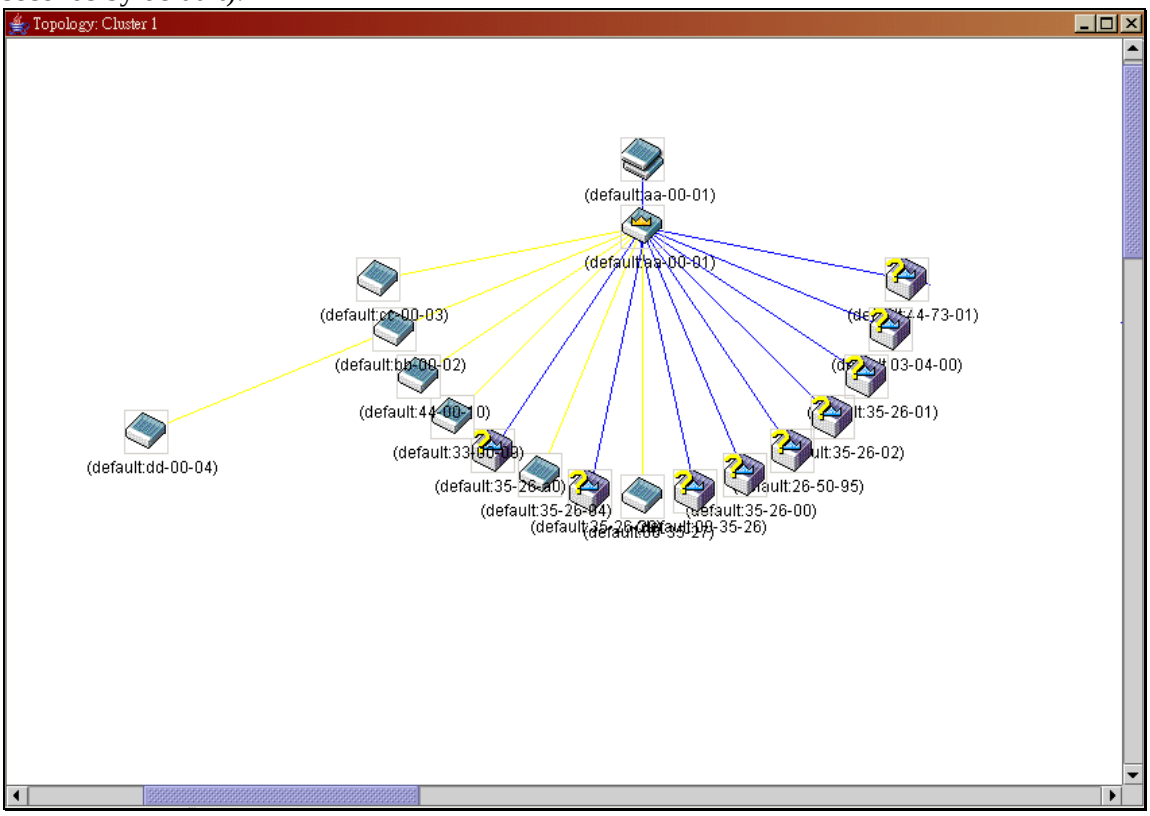



**Figure 10- 5. Topology view**

This screen will display how the devices within the **Single IP Management Group** are connected to other groups and devices. Possible icons in this screen are as follows:

| Icon | Description |
|---|---|
| | Group |
| | Layer 2 commander switch |
| | Layer 3 commander switch |
| | Commander switch of other group |
| | Layer 2 member switch. |
| | Layer 3 member switch |
| | Member switch of other group |
| | Layer 2 candidate switch |
| | Layer 3 candidate switch |
| | Unknown device |
| | Non-SIM devices |

## Tool Tips

In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Setting the mouse cursor over a specific device in the topology window (tool tip) will display the same information about a specific device as the Tree View does. See the window below for an example.

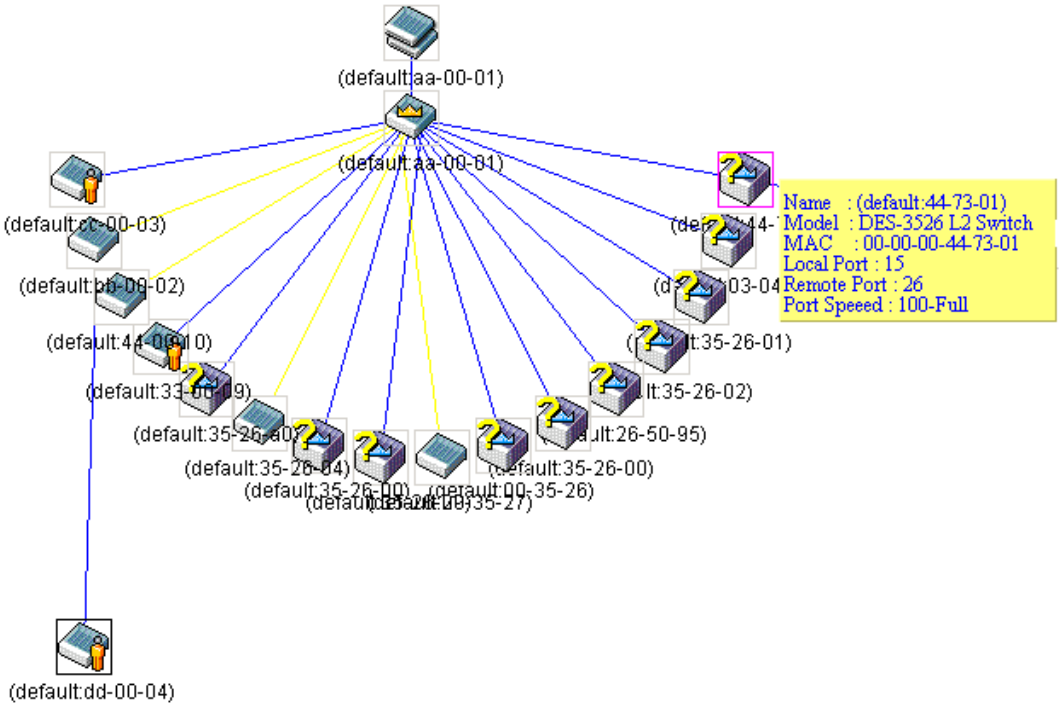



**Figure 10- 6. Device Information Utilizing the Tool Tip**

Setting the mouse cursor over a line between two devices will display the connection speed between two devices, as shown below.

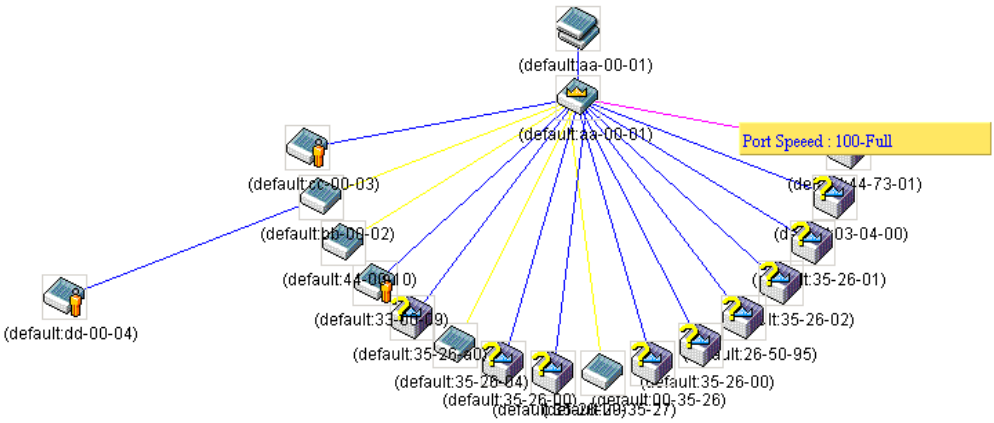



**Figure 10- 7. Port Speed Utilizing the Tool Tip**

## Right Click

Right clicking on a device will allow the user to perform various functions, depending on the role of the Switch in the SIM group and the icon associated with it.

### Group Icon

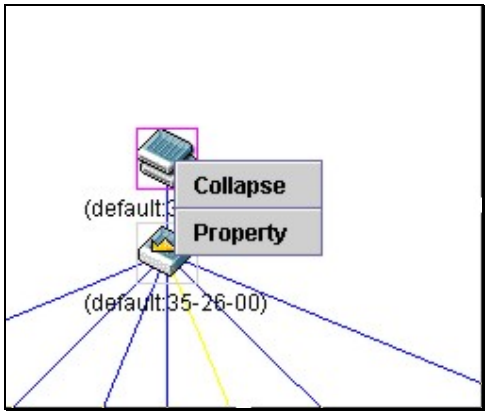



**Figure 10- 8. Right Clicking a Group Icon**

The following options may appear for the user to configure:

**Collapse** - To collapse the group that will be represented by a single icon.
**Expand** - To expand the group in detail. CS, MS, and CaS in this group are shown.
**Property** - To pop up a window to display the group information.

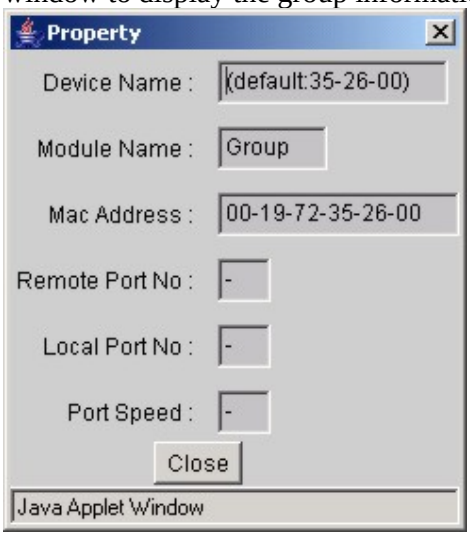



**Figure 10- 9. Property window**

### Commander Switch Icon

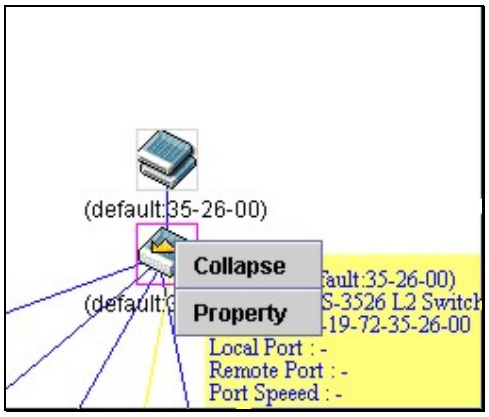



**Figure 10- 10. Right Clicking a Commander Icon**

The following options may appear for the user to configure:

**Collapse** - To collapse the group that will be represented by a single icon.
**Expand** - To expand the group in detail. CS, MS. and CaS in this group are shown.
**Configure** - Launch the web management to configure the Switch.
**Property** - To pop up a window to display the group information.

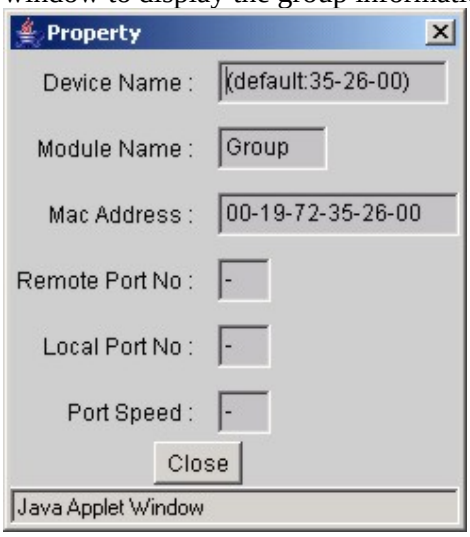



**Figure 10- 11. Property window**

### Member Switch Icon

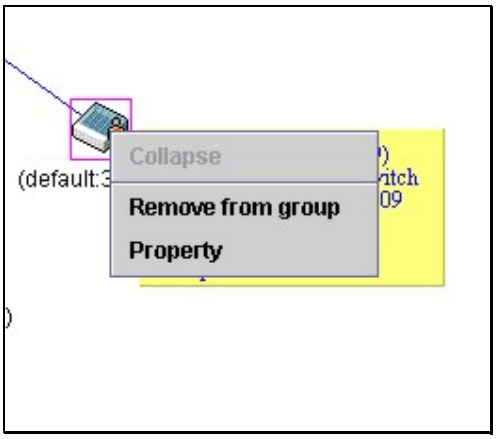



**Figure 10- 12. Right Clicking a Member icon**

The following options may appear for the user to configure:

**Remove from group** - Remove a member from a group.

**Configure** - Launch the web management to configure the Switch.

**Property** - To pop up a window to display the device information.

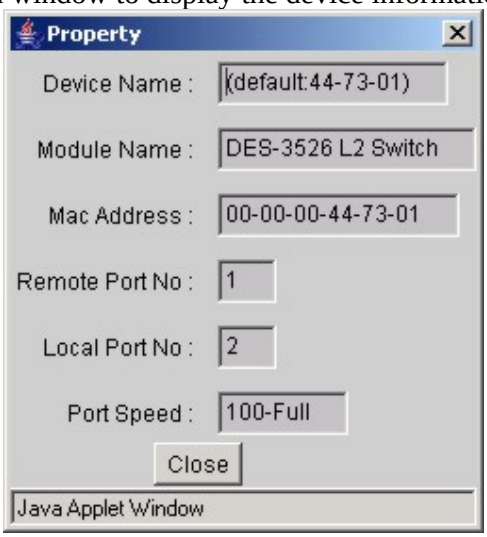



**Figure 10- 13. Property window**

### Candidate Switch Icon

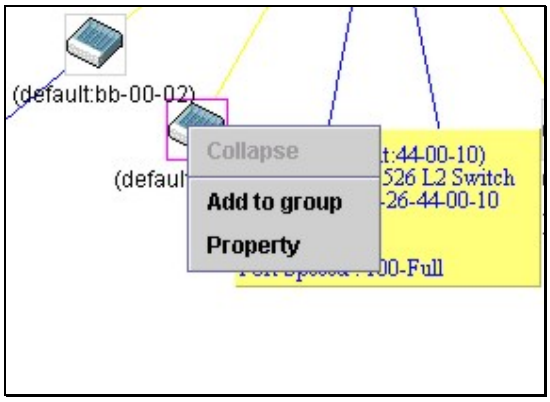



**Figure 10- 14. Right Clicking a Candidate icon**

The following options may appear for the user to configure:

**Add to group** - Add a candidate to a group. Clicking this option will reveal the following screen for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click *OK* to enter the password or *Cancel* to exit the window.

**Figure 10- 15. Input password window.**

**Property** - To pop up a window to display the device information, as shown below.

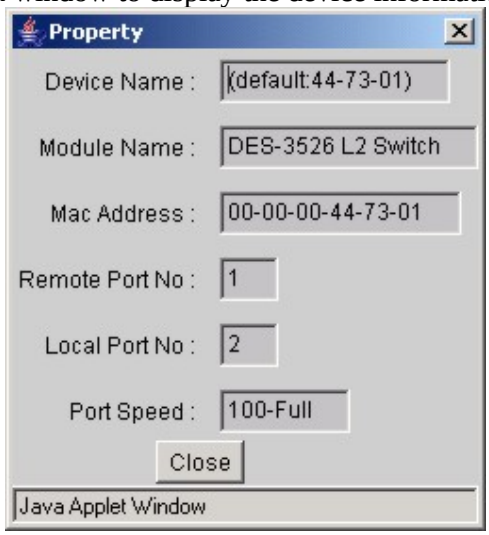



**Figure 10- 16. Device Property window.**

This window holds the following information:

| Parameter | Description |
|---|---|

| | |
|---|---|
| **Device Name** | This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it. |
| **Local Port** | Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field. |
| **Speed** | Displays the connection speed between the CS and the MS or CaS. |
| **Remote Port** | Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field. |
| **MAC Address** | Displays the MAC Address of the corresponding Switch. |
| **Model Name** | Displays the full Model Name of the corresponding Switch. |

Click *Close* to close the **Property** window.

## Menu Bar

The Single IP Management window contains a menu bar for device configurations, as seen below.

**Figure 10- 17. Menu Bar of the Topology View**

The five menus on the menu bar are as follows.

### File

**Print Setup -** Will view the image to be printed.
**Print Topology**- Will print the topology map.
**Preference** - Will set display properties, such as polling interval, and the views to open at SIM startup.

### Group

**Add to group** - Add a Candidate to a group. Clicking this option will reveal the following screen for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click *OK* to enter the password or *Cancel* to exit the window.

**Figure 10- 18. Input password window.**

**Remove from Group** - Remove an MS from the group.

### Device

**Configure** – Will open the web manager for the specific device.

### View

**Refresh** - Update the views with the latest status.
**Topology** - Display the Topology view.

### Help

**About** – Will display the SIM information, including the current SIM version.

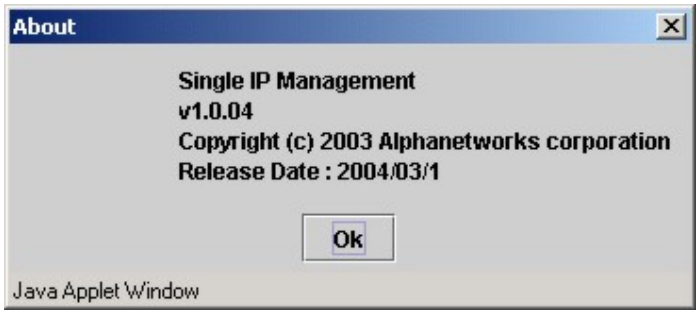



**Figure 10- 19. About window**

**NOTE:** Upon this firmware release, some functions of the SIM can only be configured through the Command Line Interface. See the ***DES-3550 Command Line Interface Reference Manual*** for more information on SIM and its configurations.

## Firmware Upgrade

This screen is used to upgrade firmware from the Commander Switch to the Member Switch. Member switches will be listed in the table and will be specified by **Port** (port on the CS where the MS resides), **MAC Address**, **Model Name**, and **Version**. To specify a certain Switch for firmware download, click its corresponding check box under the **Port** heading. To update the firmware, enter the **Server IP Address** where the firmware resides and enter the **Path/Filename** of the firmware. Click *Download* to initiate the file transfer.

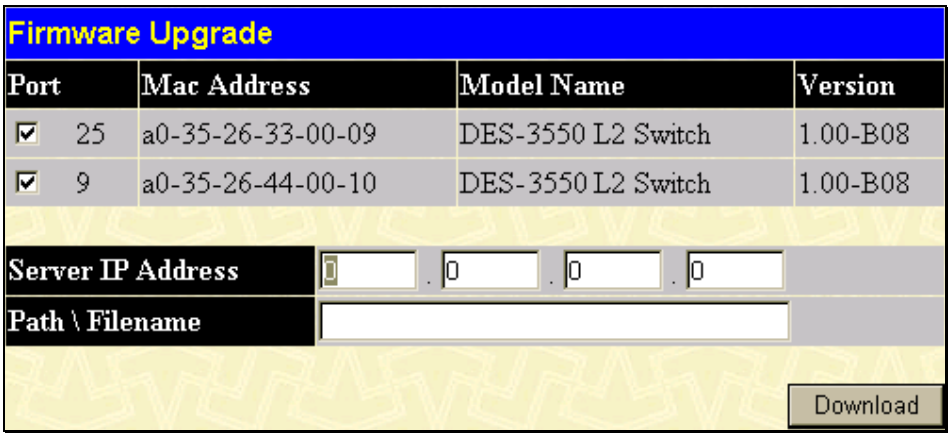



**Figure 10- 20. Firmware Upgrade window**

## Configuration File Backup/Restore

This screen is used to upgrade configuration files from the commander switch to the member switch. Member switches will be listed in the table and will be specified by **Port** (port on the CS where the MS resides), **MAC Address**, **Model Name**, and **Version**. To specify a certain Switch for upgrading configuration files, click its corresponding radio button under the **Port** heading. To update the configuration file, enter the **Server IP Address** where the firmware resides and enter the **Path/Filename** of the firmware. Click *Download* to initiate the file transfer.

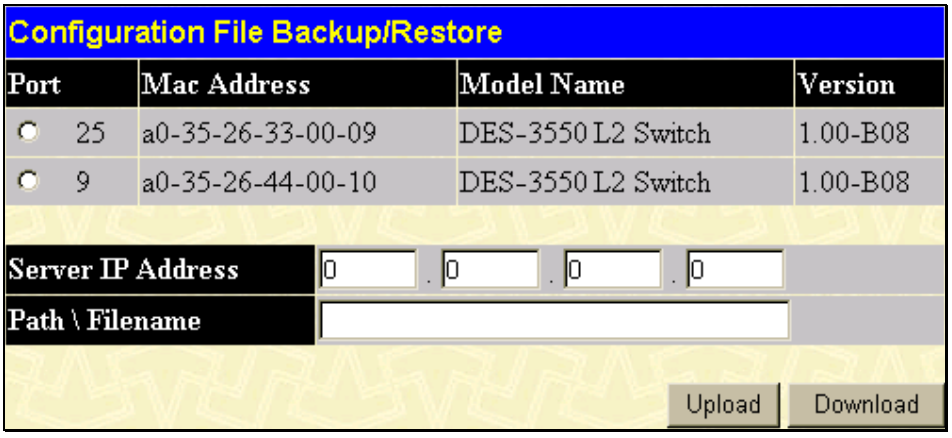



**Figure 10- 21. Configuration File Backup/Restore window**

# Appendix A

## General

| | |
|---|---|
| **Standards:** | IEEE 802.3u 100BASE-TX Fast Ethernet<br>IEEE 802.3ab 1000BASE-T Gigabit Ethernet<br>IEEE 802.1D Spanning Tree<br>IEEE 802.1W Rapid Spanning Tree<br>IEEE 802.1 P/Q VLAN<br>IEEE 802.1p Priority Queues<br>IEEE 802.3ad Link Aggregation Control<br>IEEE 802.3x Full-duplex Flow Control<br>IEEE 802.3 Nway auto-negotiation |
| **Protocols:** | CSMA/CD |
| **Data Transfer Rates:**<br><br>**Ethernet:**<br>**Fast Ethernet:**<br>**Gigabit Ethernet:** | Half-duplex Full-duplex<br><br>10 Mbps 20 Mbps<br>100 Mbps 200 Mbps<br>2000 Mbps (Full duplex only) |
| **Topology:** | Star |
| **Network Cables**<br><br>**10BASE-T:**<br><br><br><br>**100BASE-TX:**<br><br><br><br>**1000BASE-T:**<br><br><br>**1000BASE-LX:** | <br><br>UTP Category 3, 4, 5 (100 meters max.)<br>EIA/TIA- 568 150-ohm STP (100 meters max.)<br><br>UTP Cat. 5 (100 meters max.)<br>EIA/TIA-568 150-ohm STP (100 meters max.)<br><br>UTP Cat. 5e (100 meters max.)<br>UTP Cat. 5 (100 meters max.)<br>EIA/TIA-568B 150-ohm STP (100 meters max.) |

| | |
|---|---|
| **1000BASE-SX**<br><br>**1000BASE-LHX:**<br><br>**1000BASE-ZX:**<br><br>**Mini-GBIC:** | Single-mode fiber module (10km)<br><br>Multi-mode fiber module (550m)<br><br>Single-mode fiber module (40km)<br><br>Single-mode fiber module (80km)<br><br>SFP Transceiver for 1000BASE-LX<br>Single-mode fiber module (10km) |
| **Number of Ports** | 48 10/100/1000 Mbps ports<br>2 1000BASE-T Mini-GBIC Combo Ports |

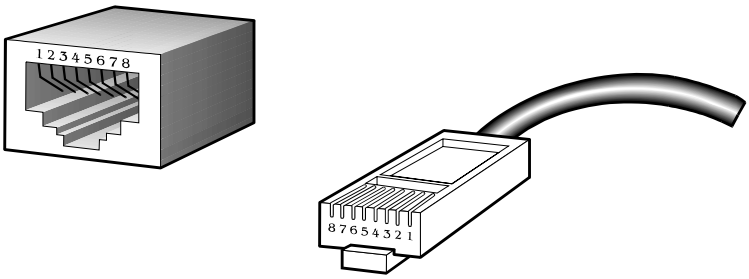
## Performance

| | |
|---|---|
| **Transmission Method:** | Store-and-forward |
| **Packet Buffer:** | 64 MB per device |
| **Packet Filtering/ Forwarding Rate:** | Full-wire speed for all connections. 1,488,095 pps per port (for 1000Mbps) |
| **MAC Address Learning:** | Automatic update. Supports 8K MAC address. |
| **Priority Queues:** | 4 Priority Queues per port. |
| **Forwarding Table Age Time:** | Max age: 10-1000000 seconds.<br>Default = 300. |

# Appendix B

## Cables and Connectors

When connecting the Switch to another switch, a bridge, or hub, a normal cable is necessary. Please review these products for matching cable pin assignment.
The following diagrams and tables show the standard RJ-45 receptacle/connector and their pin assignments.




**The standard RJ-45 port and connector**

| RJ-45 Pin Assignments | | |
|---|---|---|
| **Contact** | **MDI-X Port** | **MDI-II Port** |
| 1 | RD+ (receive) | TD+ (transmit) |
| 2 | RD- (receive) | TD- (transmit) |
| 3 | TD+ (transmit) | RD+ (receive) |
| 4 | Not used | Not used |
| 5 | Not used | Not used |
| 6 | TD- (transmit) | RD- (receive) |
| 7 | Not used | Not used |
| 8 | Not used | Not used |

**The standard RJ-45 pin assignments**

# Appendix C

## Cable Lengths

Use the following table to as a guide for the maximum cable lengths.

| Standard | Media Type | Maximum Distance |
|---|---|---|
| **Mini-GBIC** | 1000BASE-LX, Single-mode fiber module | 10km (32,808ft) |
| | 1000BASE-SX, Multi-mode fiber module | 550m (1805ft) |
| | 1000BASE-LHX, Single-mode fiber module | 40km (131,234ft) |
| | 1000BASE-ZX, Single-mode fiber module | 80km (262,467ft) |
| **1000BASE-T** | Category 5e UTP Cable<br>Category 5 UTP Cable (1000 Mbps) | 100m (328ft) |
| **100BASE-TX** | Category 5 UTP Cable (100 Mbps) | 100m (328ft) |
| **10BASE-T** | Category 3 UTP Cable (10 Mbps) | 100m (328ft) |

## Glossary

**1000BASE-LX:** A short laser wavelength on multimode fiber optic cable for a maximum length of 550 meters (1805 feet).
**1000BASE-SX:** A long wavelength for a "long haul" fiber optic cable for a maximum length of 10 kilometers (32,808 feet).
**100BASE-FX:** 100Mbps Ethernet implementation over fiber.
**100BASE-TX:** 100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.
**10BASE-T:** The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.
**ageing:** The automatic removal of dynamic entries from the Switch Database, which have timed-out and are no longer valid.

**ATM:** Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data, and video signals.
**auto-negotiation:** A feature on a port that allows it to advertise its capabilities for speed, duplex, and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.
**backbone port:** A port that does not learn device addresses, and receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.
**backbone:** The part of a network used as the primary path for transporting traffic between network segments.
**bandwidth:** Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.
**baud rate**: The switching speed of a line. Also known as *line speed* between network segments.
**BOOTP:** The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.
**bridge:** A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.
**broadcast:** A message sent to all destination devices on the network.
**broadcast storm:** Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.
**console port:** The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.
**CSMA/CD:** Channel access method used by Ethernet and IEEE 802.3 standards, in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.
**data center switching:** The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection, and a control point for network management and security.
**Ethernet:** A LAN specification developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.
**Fast Ethernet:** 100Mbps technology based on the Ethernet/CD network access method.
**Flow Control:** (IEEE 802.3z) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested switch port.
**forwarding:** The process of sending a packet toward its destination by an internetworking device.
**Full-duplex:** A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.
**Half-duplex:** A system that allows packets to be transmitted and received, but not at the same time. Contrast with *full-duplex*.

**IP address:** Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.
**IPX:** Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.
**LAN:** Local Area Network. A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.
**latency:** The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.
**line speed:** See *baud rate*.
**main port:** The port in a resilient link that carries data traffic in normal operating conditions.
**MDI:** Medium Dependent Interface. An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.
**MDI-X:** Medium Dependent Interface Cross-over. An Ethernet port connection where the internal transmit and receive lines are crossed.
**MIB:** Management Information Base. Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.
**multicast:** Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.
**protocol:** A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing, and error control.
**resilient link:** A pair of ports that can be configured so that one will take over data transmission should the other fail. See also *main port* and *standby port*.
**RJ-45:** Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.
**RMON:** Remote Monitoring. A subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.
**RPS:** Redundant Power System. A device that provides a backup source of power when connected to the Switch.
**server farm:** A cluster of servers in a centralized location serving a large user population.
**SLIP:** Serial Line Internet Protocol. A protocol that allows IP to run over a serial line connection.
**SNMP:** Simple Network Management Protocol. A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.
**Spanning Tree Protocol** (STP): A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and to ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.
**stack:** A group of network devices that are integrated to form a single logical device.
**standby port:** The port in a resilient link that will take over data transmission if the main port in the link fails.

**switch:** A device that filters, forwards, and floods packets based on the packet's destination address. The Switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.
**TCP/IP:** A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.
**telnet:** A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.
**TFTP:** Trivial File Transfer Protocol. Allows you to transfer files (such as software upgrades) from a remote device using your switch's local management capabilities.
**UDP:** User Datagram Protocol. An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.
**VLAN:** Virtual LAN. A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.
**VLT:** Virtual LAN Trunk. A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.
**VT100:** A type of terminal that uses ASCII characters. VT100 screens have a text-based appearance.

# D-Link Offices

**Australia** **D-Link Australasia**

1 Giffnock Avenue, North Ryde, NSW 2113, Sydney, Australia
TEL: 61-2-8899-1800 FAX: 61-2-8899-1868
TOLL FREE (Australia): 1300 766 868
TOLL FREE (New Zealand): 0800-900900
URL: www.dlink.com.au
E-MAIL: support@dlink.com.au & info@dlink.com.au

**Brazil** **D-Link Brasil Ltda.**

Rua Tavares Cabral 102 - Conj. 31 e 33
05423-030 Pinheiros, Sao Paulo, Brasil
TEL: (5511) 3094 2910 to 2920 FAX: (5511) 3094 2921
URL: www.dlink.com.br

**Canada** **D-Link Canada**

2180 Winston Park Drive, Oakville,
Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5223
BBS: 1-965-279-8732 FTP: ftp.dlinknet.com
TOLL FREE: 1-800-354-6522
URL: www.dlink.ca E-MAIL: techsup@dlink.ca

**Chile** **D-Link South America (Sudamérica)**

Isidora Goyenechea 2934
Oficina 702, Las Condes, Santiago, Chile
TEL: 56-2-232-3185 FAX: 56-2-232-0923
URL: www.dlink.com.cl

**China** **D-Link Beijing**

Level 5,Tower W1,The Tower,Oriental Plaza
No.1,East Chang An Ave., Dong Cheng District
Beijing,100738,China
TEL: (8610) 85182529/30/31/32/33
FAX: (8610) 85182250
URL: www.dlink.com.cn E-MAIL: webmaster@dlink.com.cn

**Denmark** **D-Link Denmark**

Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL: 45-43-969040 FAX: 45-43-424347
URL: www.dlink.dk E-MAIL: info@dlink.dk

**Egypt** **D-Link Middle East**

7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt

TEL: 202-624-4615 FAX: 202-624-583

URL: www.dlink-me.com

E-MAIL: support@dlink-me.com & dlinkegypt@dlink-me.com

**Finland** **D-Link Finland**

Pakkalankuja 7A, 01510 Vantaa, Finland

TEL: 358-9-2707-5080 FAX: 358-9-2707-5081

URL: www.dlink-fi.com

**France** **D-Link France**

Le Florilege, No. 2, Allée de la Fresnerie,

78330 Fontenay-le-Fleury, France

TEL: 33-1-3023-8688 FAX: 33-1-3023-8689

URL: www.dlink-france.fr

E-MAIL: info@dlink-france.fr

**Germany** **D-Link Central Europe (D-Link Deutschland GmbH)**

Schwalbacher Strasse 74, D-65760 Eschborn, Germany

TEL: 49-6196-77990 FAX: 49-6196-7799300

BBS: 49-(0) 6192-971199 (analog) & BBS: 49-(0) 6192-971198 (ISDN)

INFO: 00800-7250-0000 (toll free) & HELP: 00800-7250-4000 (toll free)

REPAIR: 00800-7250-8000 & HELP: support.dlink.de

URL: www.dlink.de & E-MAIL: info@dlink.de

**India** **D-Link India**

Plot No.5, Kurla -Bandra Complex Rd., Off Cst Rd.,

Santacruz (East), Mumbai, 400 098 India

TEL: 91-022-2652-6696/6788/6623

FAX: 91-022-2652-8914/8476

URL: www.dlink.co.in

E-MAIL: service@dlink.co.in & tushars@dlink.co.in

**Italy** **D-Link Mediterraneo Srl/D-Link Italia**

Via Nino Bonnet n. 6/B, 20154, Milano, Italy

TEL: 39-02-2900-0676 FAX: 39-02-2900-1723

URL: www.dlink.it E-MAIL: info@dlink.it

**Japan** **D-Link Japan**

10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141, Japan

TEL: 81-3-5434-9678 FAX: 81-3-5434-9868

URL: www.d-link.co.jp E-MAIL: kida@d-link.co.jp

**Netherlands** **D-Link Benelux**

Lichtenauerlaan 102-120, 3062 ME Rotterdam, Netherlands
TEL: +31-10-2045740 FAX: +31-10-2045880
URL: www.d-link-benelux.nl & www.dlink-benelux.be
E-MAIL: info@dlink-benelux.com

**Norway** **D-Link Norway**

Karihaugveien 89, 1086 Oslo
TEL: 47-22-309075 FAX: 47-22-309085
SUPPORT: 800-10-610 & 800-10-240 (DI-xxx)
URL: www.dlink.no

**Russia** **D-Link Russia**

129626 Russia, Moscow, Graphskiy per., 14, floor 6
TEL/FAX: +7 (095) 744-00-99
URL: www.dlink.ru E-MAIL: vl@dlink.ru

**Singapore** **D-Link International**

1 International Business Park, #03-12 The Synergy,
Singapore 609917
TEL: 65-6774-6233 FAX: 65-6774-6322
E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com

**South Africa** **D-Link South Africa**

Einstein Park II, Block B, 102-106 Witch-Hazel Avenue
Highveld Technopark
Centurion, Gauteng, Republic of South Africa
TEL: +27-12-665-2165 FAX: +27-12-665-2186
URL: www.d-link.co.za E-MAIL: attie@d-link.co.za

**Spain** **D-Link Iberia S.L.**

Sabino de Arana, 56 bajos, 08028 Barcelona, Spain
TEL: 34 93 409 0770 FAX: 34 93 491 0795
URL: www.dlink.es E-MAIL: info@dlink.es

**Sweden** **D-Link Sweden**

P. O. Box 15036, S-167 15 Bromma, Sweden
TEL: 46-8-564-61900 FAX: 46-8-564-61901
URL: www.dlink.se E-MAIL: info@dlink.se

**Taiwan** **D-Link Taiwan**

2F, No. 119, Pao-chung Road, Hsin-tien, Taipei, Taiwan
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw E-MAIL: dssqa@dlinktw.com.tw

**Turkey** **D-Link Turkiye**

Beybi Giz Plaza, Ayazaga Mah. Meydan Sok. No. 28
Maslak 34396, Istanbul-Turkiye
TEL: 90-212-335-2553 (direct) & 90-212-335-2525 (pbx)
FAX: 90-212-335-2500 E-MAIL: dlinkturkey@dlink-me.com
E-MAIL: support@dlink-me.com

**U.A.E.** **D-Link Middle East FZCO**

P.O. Box18224 R/8, Warehouse UB-5
Jebel Ali Free Zone, Dubai – United Arab Emirates
TEL: (Jebel Ali): 971-4-883-4234
FAX: (Jebel Ali): 971-4-883-4394 & (Dubai): 971-4-335-2464
E-MAIL: dlinkme@dlink-me.com & support@dlink-me.com

**U.K.** **D-Link Europe (United Kingdom) Ltd**

4th Floor, Merit House, Edgware Road, Colindale, London
NW9 5AB United Kingdom
TEL: 44-020-8731-5555 SALES: 44-020-8731-5550
FAX: 44-020-8731-5511 SALES: 44-020-8731-5551
BBS: 44 (0) 181-235-5511
URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

**U.S.A.** **D-Link U.S.A.**

17595 Mt. Hermmann, Fountain Valley, CA 92708-4160, USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033
INFO: 1-800-326-1688 URL: www.dlink.com
E-MAIL: tech@dlink.com & support@dlink.com

# Warranty and Registration for all Countries and Regions Except USA

## Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sint beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.
    c. Das Gerät war Feuchtigkeit ausgesetzt.
    d. Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

## WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS.

D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

## LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

## Limited Warranty

### Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.
This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.
If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.
Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.
After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.
Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

## Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.
D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

D-Link®
Building Networks for People

## Limited Warranty
(USA Only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

- D-Link or its authorized reseller or distributor and
- Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

***Limited Warranty:*** D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type ("Warranty Period"), except as otherwise stated herein.

Limited Lifetime Warranty for the Product(s) is defined as follows:

- Hardware for as long as the original customer/end user owns the product, or five years after product discontinuance, whichever occurs first (excluding power supplies and fans)
- Power Supplies and Fans Three (3) Year
- Spare parts and spare kits Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

***Limited Software Warranty:*** D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund at D-Link's sole discretion. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Software will be warranted for the remainder of the original Warranty Period from the date or original retail purchase. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

***Non-Applicability of Warranty:*** The Limited Warranty provided hereunder for hardware and software of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

***Submitting A Claim***: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.

The original product owner must obtain a Return Material Authorization ("RMA") number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.

The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

***What Is Not Covered:*** This limited warranty provided by D-Link does not cover: Products, if in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

***Disclaimer of Other Warranties:*** EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE

ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

***Limitation of Liability:*** TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY

***Governing Law***: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

**Trademarks:** D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective manufacturers or owners.

**Copyright Statement:** No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice. Copyright© 2005 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

**CE Mark Warning:** This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

**FCC Statement:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures**:**

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**For detailed warranty outside the United States, please contact corresponding local D-Link office.**

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.